



## ADMINISTRATION GUIDE

Cisco Small Business Pro  
ESW 500 Series Switches



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

 CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

<b>Chapter : Getting Started</b>	<b>12</b>
Introduction	12
Typical Installation Methods	13
Default Configuration settings on the ESW 500 Series Switches	14
Physical Connectivity	14
Connecting to the Switch	17
Using the Default Static IP Address	17
Using a Dynamic IP Address Allocated to the Switch By DHCP	22
Using the Cisco Configuration Assistant (CCA)	24
Navigating The Cisco Switch Configuration Utility	29
Using the Management Buttons	29
Performing Common Configuration Tasks	30
Checking the Software Version	30
Checking the System Information	30
Viewing what Devices are Attached to the Switch	31
Configuring the VLAN Settings for the Switch	32
Configuring individual ports using Cisco Smartport Roles	33
Smartport Roles	34
Checking the Device Power Consumption	38
Saving the Configuration	40
Upgrading the Firmware on the Switch	41
Resetting the Device	46
Manual Reset	47
Logging Off the Device	47
Using The Switch Console Port	48
Selecting Menu Options and Actions	48
 <b>Chapter : Managing Device Information</b>	 <b>52</b>
Understanding the Dashboards	52
Ports	59
Health and Monitoring	59
Common Tasks	60

Help	60
Defining System Information	60
Viewing Device Health	62
Resetting the Device	64
Managing Cisco Discovery Protocol	65
Defining the Bonjour Discovery Protocol	68
TCAM Utilization	70
<b>Chapter : Managing Smart Ports</b>	<b>72</b>
Configuring Smart Ports for Desktops	73
Configuring Smart Ports for IP Phones and Desktops	77
Configuring Smart Ports for Access Points	80
Configuring Smart Ports for Switches	82
Configuring Smart Ports for Routers	84
Configuring Smart ports for Guests	87
Configuring Smart ports for Servers	89
Configuring Smart ports for Printers	91
Configuring Smart ports for VS Camera	94
Configuring Smart Ports for Other	96
<b>Chapter : Configuring System Time</b>	<b>99</b>
Defining System Time	99
Defining SNTP Settings	103
Defining SNTP Authentication	105
<b>Chapter : Configuring Device Security</b>	<b>108</b>
Passwords Management	108
Modifying the Local User Settings	110
Defining Authentication	111
Defining Profiles	111
Modifying an Authentication Profile	114

Mapping Authentication Profiles	115
Defining TACACS+	117
Modifying TACACS+ Settings	120
Defining RADIUS	122
Modifying RADIUS Server Settings	126
Defining Access Methods	127
Defining Access Profiles	128
Defining Profile Rules	131
Modifying Profile Rules	135
Defining Traffic Control	137
Defining Storm Control	138
Modifying Storm Control	140
Defining Port Security	141
Modifying Port Security	145
Defining 802.1x	146
Defining 802.1X Properties	147
Defining Port Authentication	149
Modifying 8021X Security	152
Defining Authentication	155
Modifying Authentication Settings	157
Authenticated Hosts	158
Defining Access Control	160
Defining MAC Based ACL	160
Adding Rule to MAC Based ACL	164
Modifying MAC Based ACL	166
Defining IP Based ACL	168
Modifying IP Based ACL	174
Adding an IP Based Rule	177
Defining ACL Binding	179
Modifying ACL Binding	180
Defining DoS Prevention	181
DoS Global Settings	181

Defining Martian Addresses	183
Defining DHCP Snooping	185
Defining DHCP Snooping Properties	186
Defining DHCP Snooping on VLANs	188
Defining Trusted Interfaces	189
Binding Addresses to the DHCP Snooping Database	191
Query By	192
Query Results	193
Defining IP Source Guard	195
Configuring IP Source Guard Properties	195
Defining IP Source Guard Interface Settings	197
Querying the IP Source Binding Database	199
TCAM Resources	200
Query By	201
Query Results	201
Defining Dynamic ARP Inspection	202
Defining ARP Inspection Properties	203
Defining ARP Inspection Trusted Interfaces	205
Defining ARP Inspection List	207
Static ARP Inspection Table	208
Adding a Binding List entry	209
Assigning ARP Inspection VLAN Settings	210
Enabled VLAN Table	211

## Chapter : Configuring Ports 213

Port Settings	213
Modifying Port Settings	215

## Chapter : Configuring VLANs 219

Defining VLAN Properties	220
Modifying VLANs	222
Defining VLAN Membership	223
Modifying VLAN Membership	224

Assigning Ports to Multiple VLANs	226
Defining Interface Settings	229
Modifying VLAN Interface Settings	230
Defining GVRP Settings	232
Modifying GVRP Settings	234
Defining Protocol Groups	236
Modifying Protocol Groups	237
Defining a Protocol Port	238
<b>Chapter : Configuring IP Information</b>	<b>241</b>
IP Addressing	241
Defining DHCP Relay	243
Defining DHCP Relay Interfaces	245
Managing ARP	247
ARP Table	249
Modifying ARP Settings	250
Domain Name System	251
Defining DNS Servers	251
Default Parameters	252
DNS Server Details	253
Mapping DNS Hosts	253
<b>Chapter : Defining Address Tables</b>	<b>256</b>
Defining Static Addresses	256
Defining Dynamic Addresses	259
Query By Section	261
<b>Chapter : Configuring Multicast Forwarding</b>	<b>262</b>
IGMP Snooping	262
Modifying IGMP Snooping	264
Defining Multicast Group	266

Modifying a Multicast Group	268
Defining Multicast Forwarding	269
Modifying Multicast Forwarding	271
Defining Unregistered Multicast Settings	272

## Chapter : Configuring Spanning Tree 275

Defining STP Properties	275
Global Settings	276
Defining Spanning Tree Interface Settings	278
Modifying Interface Settings	282
Defining Rapid Spanning Tree	284
Modifying RTSP	287
Defining Multiple Spanning Tree	289
Defining MSTP Properties	290
Defining MSTP Instance to VLAN	291
Defining MSTP Instance Settings	293
Defining MSTP Interface Settings	294

## Chapter : Configuring Quality of Service 301

Managing QoS Statistics	302
Policer Statistics	302
Add Aggregated Policer Statistics	304
Resetting Aggregate Policer Statistics Counters	307
Queues Statistics	307
Adding Queues Statistics	309
Resetting Queue Statistics Counters	309
Defining General Settings	310
Defining CoS	310
Modifying Interface Priorities	312
Defining QoS Queue	313
Mapping CoS to Queue	316
Mapping DSCP to Queue	318



Configuring Bandwidth	319
Modifying Bandwidth Settings	320
Configuring VLAN Rate Limit	322
Modifying the VLAN Rate Limit	324
Defining Advanced QoS Mode	324
Configuring DSCP Mapping	325
Defining Class Mapping	327
Defining Aggregate Policer	329
Modifying QoS Aggregate Policer	331
Configuring Policy Table	332
Modifying the QoS Policy Profile	335
Defining Policy Binding	337
Modifying QoS Policy Binding Settings	339
Defining QoS Basic Mode	340
Rewriting DSCP Values	341

## Chapter : Configuring SNMP 343

SNMP Versions	343
SNMP v1 and v2	343
SNMP v3	343
Configuring SNMP Security	344
Defining the SNMP Engine ID	344
Defining SNMP Views	346
Defining SNMP Users	348
Modifying SNMP Users	350
Define SNMP Groups	351
Modifying SNMP Group Profile Settings	354
Defining SNMP Communities	355
Modifying SNMP Community Settings	358
Defining Trap Management	359
Defining Trap Settings	359
Configuring Station Management	361

Modifying SNMP Notifications	365
Defining SNMP Filter Settings	367
Managing Cisco Discovery Protocol	370
<b>Chapter : Managing System Files</b>	<b>373</b>
Software Upgrade	374
Save Configuration	375
Copy Configuration	377
Via TFTP	378
Via HTTP	379
Active Image	379
DHCP Auto Configuration	381
<b>Chapter : Managing Power-over-Ethernet Devices</b>	<b>382</b>
Defining PoE Settings	382
<b>Chapter : Managing System Logs</b>	<b>386</b>
Enabling System Logs	386
Viewing the Device Memory Logs	388
Clearing Message Logs	389
Viewing the System Flash Logs	390
Clearing Flash Logs	391
Remote Log Servers	391
Modifying Syslog Server Settings	394
<b>Chapter : Viewing Statistics</b>	<b>397</b>
Viewing Ethernet Statistics	397
Defining Interface Statistics	397
Resetting Interface Statistics Counters	399
Viewing Etherlike Statistics	399
Resetting Etherlike Statistics Counters	401
Viewing GVRP Statistics	401

Resetting GVRP Statistics Counters	403
Viewing EAP Statistics	403
Managing RMON Statistics	405
Viewing RMON Statistics	406
Resetting RMON Statistics Counters	408
Configuring RMON History	408
Defining RMON History Control	408
Viewing the RMON History Table	411
Defining RMON Events Control	413
Modifying RMON Event Log Settings	415
Viewing the RMON Events Logs	416
Defining RMON Alarms	417
Modifying RMON Alarm Settings	421

## Chapter : Aggregating Ports 424

Defining EtherChannel Management	425
Defining EtherChannel Settings	427
Modifying EtherChannel Settings	429
Configuring LACP	431

## Chapter : Managing Device Diagnostics 434

Ethernet Port Testing	434
Performing GBIC Uplink Testing	437
Configure Span (Port Mirroring)	438
Monitoring CPU Utilization	440

# Getting Started

## Introduction

Thank you for choosing the Cisco Small Business Pro ESW 500 Series Switch. The ESW 500 series is a family of Ethernet switches that addresses network infrastructure and access needs of small business customers for voice, data, PCs, Servers, and video applications. They are simple to deploy and manage for use with IP phones, Access Points, IP cameras, and Network Attached Storage servers as well as most any Ethernet device. The ESW 500 series includes seven Fast Ethernet and GigE switches in both 24- and 48-port configurations with PoE and non-PoE options. The ESW 500 series also includes two 8 port PoE switches in Fast Ethernet and GigE models. The switch models covered in this guide are:

ESW 500 Series Switch	Port Configuration
ESW 520-8P	8 Port 10/100 PoE
ESW 540-8P	8 Port 10/100/1000 PoE
ESW 520-24	24 Port 10/100
ESW 520-24P	24 Port 10/100 PoE
ESW 520-48	48 Port 10/100
ESW 520-48P	48 Port 10/100 PoE
ESW 540-24	24 Port 10/100/1000
ESW 540-24P	24 Port 10/100/1000 PoE
ESW-540-48	48 Port 10/100/1000

This section provides information about the different methods to connect to the switch, as well as some examples of a typical installation. It also provides an introduction to the user interface, and includes the following:

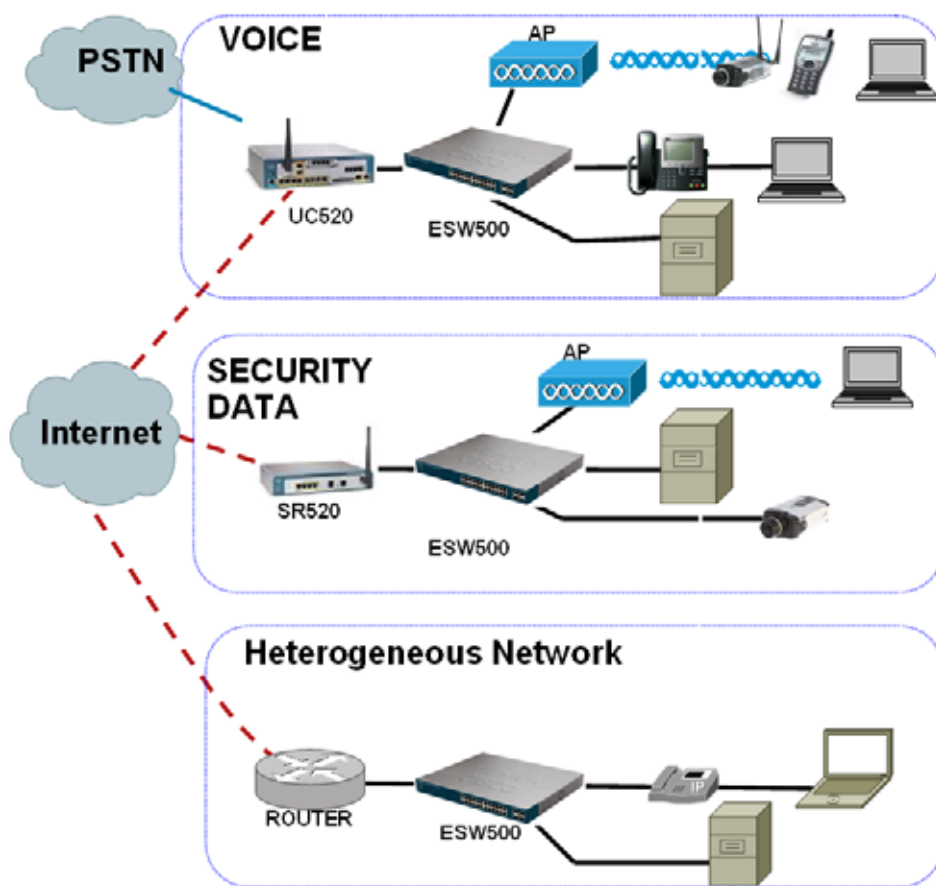
- [Typical Installation Methods, page 13](#)
- [Connecting to the Switch, page 17](#)
  - [Using the Default Static IP Address, page 17](#)
  - [Using a Dynamic IP Address Allocated to the Switch By DHCP, page 22](#)
  - [Using the Cisco Configuration Assistant \(CCA\), page 24](#)
- [Navigating The Cisco Switch Configuration Utility, page 29](#)

- [Performing Common Configuration Tasks, page 30](#)
- [Using The Switch Console Port, page 48](#)

## Typical Installation Methods

The first step in any installation scenario is to connect to the switch and configure basic connectivity to ensure it communicates with the rest of the network.

The following diagram illustrates three common installation scenarios:



In the first two scenarios, called VOICE and SECURITY DATA, you are adding an ESW 500 switch to a new or existing Cisco Smart Business Communications Systems (SBCS) network deployment. This deployment is either a VOICE network with UC520 being the anchor device or SECURITY / DATA network with the SR520 being the anchor device.

In the third scenario, called Heterogeneous Network, you are adding an ESW 500 switch to a network which does not have any Cisco Small Business products.

## Default Configuration settings on the ESW 500 Series Switches

The ESW 500 series switches ship with a default configuration that enables simplified installation and plug and play when connected into a Cisco Small Business network such as SBCS. The default settings are as follows:

- Management VLAN is VLAN 1
- Management IP Address is obtained via DHCP by default. If the switch times out on a Dynamic Host Configuration Protocol (DHCP) response, it falls back to a static IP address 192.168.10.2 with subnet mask of 255.255.255.0.
- Voice VLAN is VLAN 100
- Cisco Discovery Protocol (CDP) is enabled on all ports

## Physical Connectivity

Physical connections to the switch are described in the tables and graphics on the next two pages.

ESW 500 Series Switch	Uplink Ports		Layer 2 Ethernet Ports
	Copper	SFP (mini-GBIC)	
ESW 520-8P	GE1	GE1	1-8
ESW 540-8P	GE1	GE1	1-8
ESW 520-24/24P	GE1-GE4	GE3-GE4	1-24
ESW 520-48/48P	GE1-GE2	GE3-GE4	1-48
ESW 540-24/24P	11-12, 23-24	GE1-GE4	1-10, 13-22
ESW 540-48	23-24, 47-48	GE1-GE4	1-22, 25-46



**NOTE** On the 8 port devices, the Uplink and the GBIC ports can not be used at the same time.

The ESW 540-24/24P and ESW 540-48 use shared ports. When connecting to uplink ports, the GE ports take precedence over the Copper ports. For example, on an ESW 540-24, if you plug a device into GE1, you cannot use port 11. The other port relationships are shown in the following table:

ESW 500 Series Switch	GE Port	Takes Precedence Over Copper Port
ESW 540-24/24P	GE1	11
ESW 540-24/24P	GE2	23
ESW 540-24/24P	GE3	12
ESW 540-24/24P	GE4	24
ESW 540-48	GE1	23
ESW 540-48	GE2	47
ESW 540-48	GE3	24
ESW 540-48	GE4	48

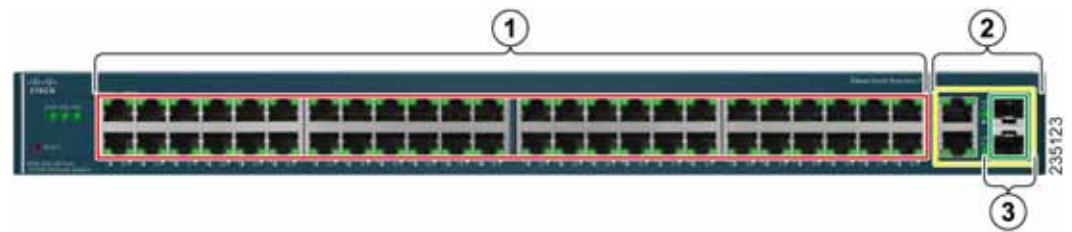
Compare the following table with the four examples of switch front panels that are on the next page:

#	Port	Description
1	Switch Ports	The switch is equipped with auto-sensing, Ethernet (802.3) network ports which use RJ-45 connectors. The Ethernet ports support network speeds of 10 Mbps, 100 Mbps, or 1000 Mbps. They can operate in half and full-duplex modes. Auto-sensing technology enables each port to automatically detect the speed of the device connected to it, and adjust its speed and duplex accordingly. These ports are typically used for devices such as PCs, servers, IP phones and Access Points., and are highlighted <b>RED</b> in the examples.
2	Uplink Ports	These ports are typically used for connecting to other switches, routers, or network backbone devices, and are highlighted in <b>YELLOW</b> in the examples. The mini-GBIC ports are a type of uplink port.
3	mini-GBIC Ports	The mini-GBIC (Gigabit Interface Converter) port is a connection point for a mini-GBIC expansion module, allowing the switch to be uplinked via fiber to another switch. Each mini-GBIC port provides a link to a high-speed network segment or individual workstation at speeds of up to 1000 Mbps. The mini-GBIC ports are highlighted in <b>GREEN</b> in the examples.

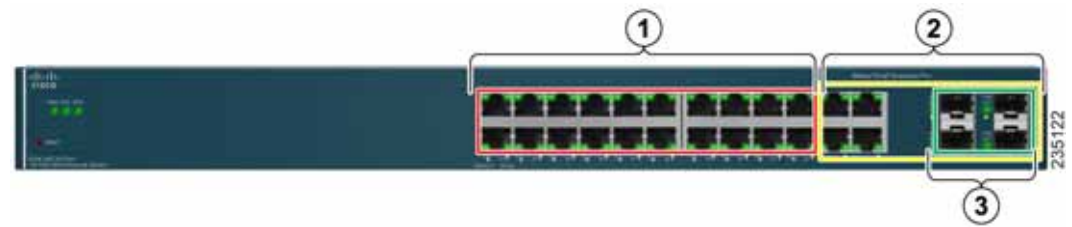
### ESW-520-24/24P



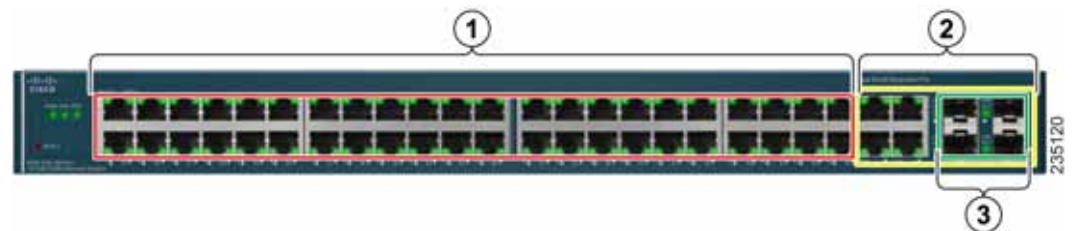
### ESW-520-48/48P



### ESW-540-24/24P



### ESW-540-48





## Connecting to the Switch

This section contains information for starting the *Switch Configuration Utility* to provision the switch features. There are four different options to connect to the switch, three of which launch the *Switch Configuration Utility*. They are:

- Using the default static IP address of the switch
- Using Cisco Configuration Assistant
- Using a dynamic IP address allocated to the switch via DHCP (from DHCP server)
- Using the Console

The first three options to connect to the switch will open the ESW 500 Series Switch Configuration Utility, which is a web-based device manager used to provision the switch. The console option uses a terminal emulation program such as HyperTerminal (bundled with Windows) or Putty (freeware).



**NOTE** Using the Console does not launch the Switch Configuration Utility and is recommended for advanced users only. Using the Console is discussed at the end of this chapter.

### Using the Default Static IP Address

To start configuring the switch, follow these steps:

- STEP 1** Make sure that there are no devices connected to the switch, the switch is not connected to the network, and then power up the switch by connecting the power cord.



**NOTE** If the switch was previously connected to the network, it may have obtained an IP address from a DHCP server. To perform a static IP address installation, disconnect all devices and remove the switch from the network. Then perform a power cycle of the switch by unplugging the power cable, waiting 5 seconds, and plugging it back in.

- STEP 2** Connect a PC to port 1 of the switch with an ethernet cable.

- STEP 3** If your PC is using a static IP address, make note of your current IP address settings, and record them for future use.
- STEP 4** Place the PC on the same subnet of the switch by configuring the PC with the following parameters:
- Static IP address — 192.168.10.11
  - Subnet mask — 255.255.255.0
  - Default gateway — 192.168.10.2



**NOTE** Details on how to change the IP address on your PC are dependent upon the type of architecture and operating system installed. Use your PC's local Help and Support functionality and search for "IP Addressing".

- STEP 5** Open a web browser. Cisco recommends Internet Explorer version 6 or higher, or Firefox version 3. Accept any requests to install Active-X plugin.

Enter **http://192.168.10.2** in the address bar and press **Enter**. The *Log In* page opens:

#### Log In page



- STEP 6** Enter a user name and password. The default user name is *cisco* and the default password is *cisco*. Passwords are both case sensitive and alpha-numeric. Click **Log In**.
- STEP 7** While the system is verifying the login attempt, the Log In Progress Indicator appears. The indicator dots rotate clockwise to indicate that the system is still working. If the login attempt is successful, the Change Username/Password Page opens.



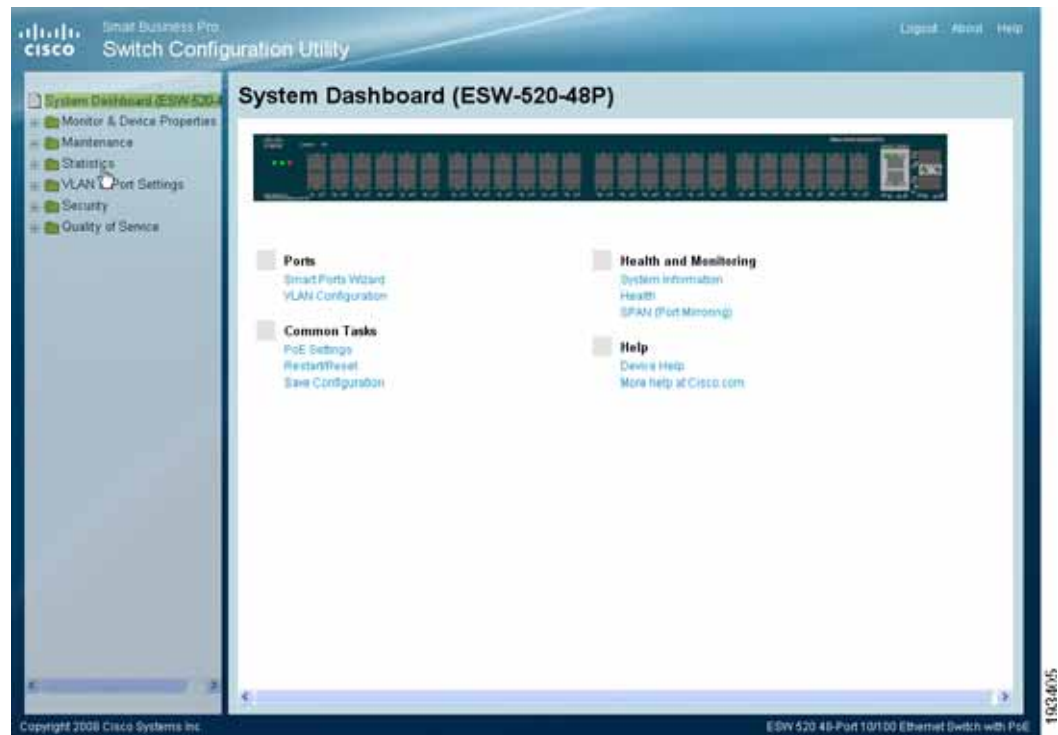
**NOTE** After logging in using the default username and password you must change to a new username and password. Only after the change has been made, can you operate the device through the web browser. Every time you log in using *cisco* as the username and password, you will be redirected to the Change Username/Password Page.

- STEP 8** Click **Apply**. The *Switch Configuration Utility - System Dashboard* Page opens.

## Getting Started

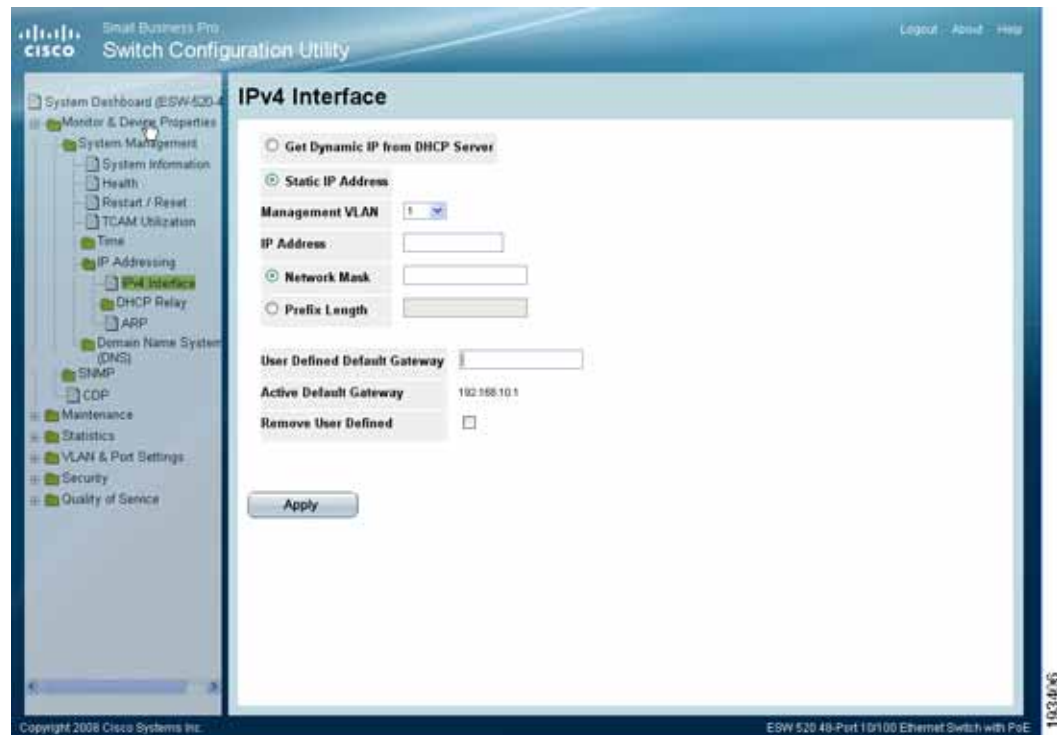
### Connecting to the Switch

#### Switch Configuration Utility - System Dashboard



- STEP 9** Click **Monitor & Device Properties > System Management > IP Addressing > IPv4 Interface**. The *IPv4 Interface* page opens.

#### IPv4 Interface Page



**NOTE** It is expected that the IP address to be assigned to the switch is known prior to installation, based on the network topology.

**STEP 10** Select the **Static IP address** radio button and enter the IP Address, Network Mask and User Defined Default Gateway. These must match the IP addressing subnet in the network in which the ESW 500 switch will be deployed. Click **Apply**.



**NOTE** The PC loses the connection to the switch at this point.

**STEP 11** Now that you have finished using the PC to connect to the switch and made the switch part of your network, you can reconfigure the PC to its original IP address configuration and physical configuration as part of your network.

**STEP 12** You are now ready to proceed with additional switch configuration.



**NOTE** If you will be using this PC for further switch configuration, it will need to be on the same subnet as the switch.

## Using a Dynamic IP Address Allocated to the Switch By DHCP

If this method of obtaining an IP address is used, you will need to have access to a configuration device that would allow you to see what IP addresses the DHCP server allocates. Prior to choosing this method of installation, speak with your network administrator to ensure you will have the correct information available to you.



**NOTE** By default, the IP address of the device is assigned dynamically.

Log on to the DHCP server and check the IP address corresponding to the Media Access Control (MAC) address of the switch. On the 24 and 48 port models, the MAC address is on the back panel of the switch next to the power adapter. On the 8 port models, the MAC address is on the bottom of the device. The illustration below shows a MAC address of 00211BFE7218.



Once you have the correct IP address that has been assigned to the switch, you can begin configuring the switch.

**STEP 1** Open a web browser. Cisco recommends Internet Explorer version 6 or higher, or Firefox version 3 or higher.

Enter the IP address that has been assigned to the switch in the address bar and press **Enter**. The *Log In* page opens:

## Getting Started

### Connecting to the Switch

#### Log In page

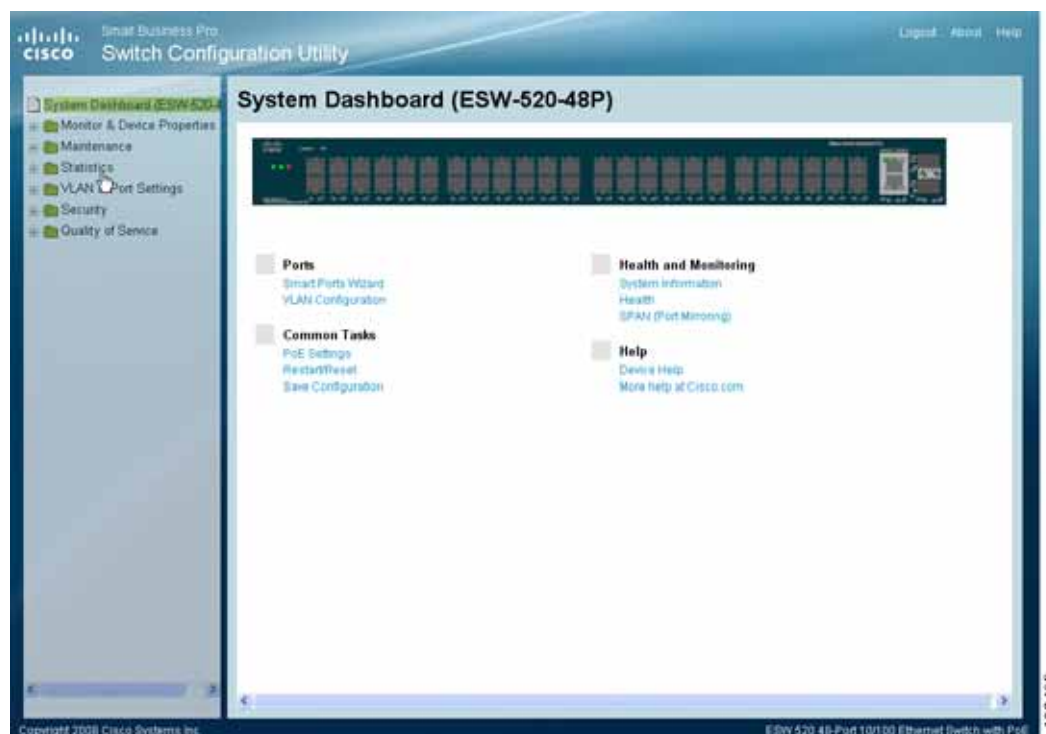


- STEP 2** Enter a user name and password. The default user name is *cisco* and the default password is *cisco*. Passwords are both case sensitive and alpha-numeric.
- STEP 3** Click **Log In**. The *Switch Configuration Utility - System Dashboard* Page opens.
- STEP 4** A window opens that prompts you to change your username and password from the default. Choose a new username and password, then click **Apply**.

## Getting Started

### Connecting to the Switch

#### Switch Configuration Utility - System Dashboard



**STEP 5** You are now ready to proceed with additional switch configuration.

#### Using the Cisco Configuration Assistant (CCA)



**NOTE** To perform an installation using CCA, you must have a PC with Windows Vista Ultimate or Windows XP, Service Pack 1 or later installed and CCA version 2.2 or higher installed.

The Cisco Configuration Assistant can be used to connect to and configure the switch when there is an existing or new Smart Business Communications System (SBCS) or with other Cisco Small Business Pro products such as the SA 500 Series Security Appliance or the AP 541 Access Point. The ESW 500 series switch obtains the management IP address via DHCP after it is connected to the network.

To begin installing the switch using CCA, perform the following steps:

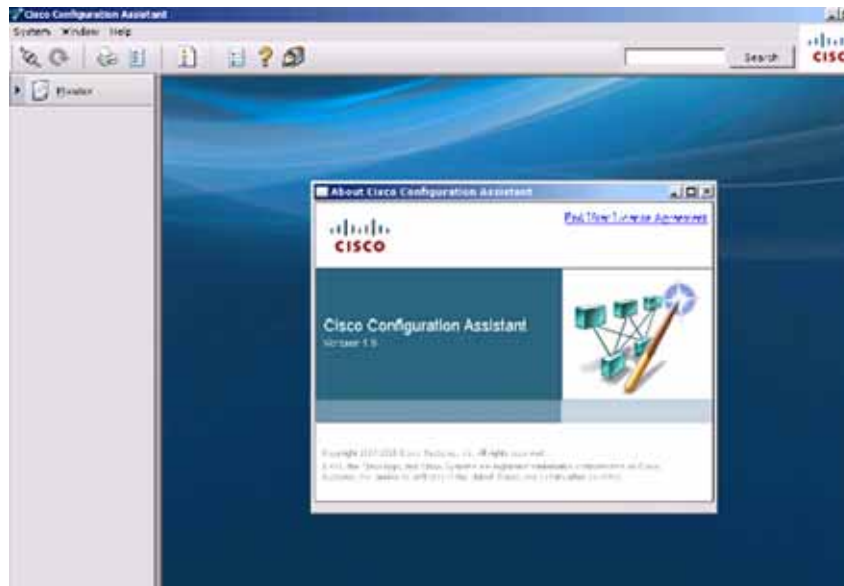


## Getting Started

### Connecting to the Switch

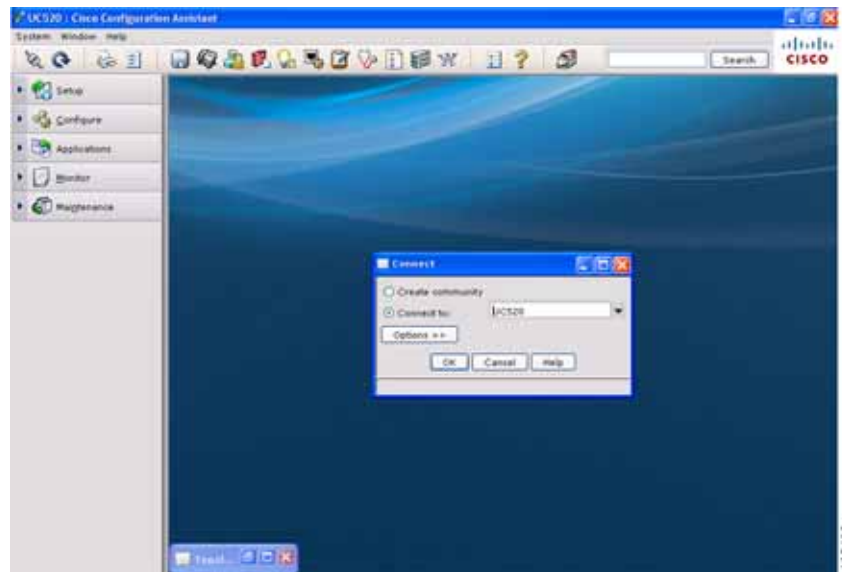
- STEP 1** Power on the ESW 500 series switch.
- STEP 2** Connect one of the designated uplink ports on the ESW 500 series switch to the expansion port on the UC520 or one of the switch ports on the SR520.
- STEP 3** Connect the PC with CCA installed to any access switch port on the ESW 500 or alternately, the UC500 or Small Business Pro router.
- STEP 4** Launch CCA. To verify you have CCA version 2.2 or higher, click **Help > About**. The *version page* opens.

#### CCA Version page



- STEP 5** Connect to an existing community, or create a new one. For more information on how to create a community, refer to the "How to create a CCA community" VOD at [https://www.myciscocommunity.com/docs/DOC-1423#UC500\\_System\\_Level\\_Features](https://www.myciscocommunity.com/docs/DOC-1423#UC500_System_Level_Features)

#### Connect page



**STEP 6** Once you have connected to the community, the *Topology View* opens and displays the ESW 500 Series Switch. **Right-click** on the switch and it displays three options:

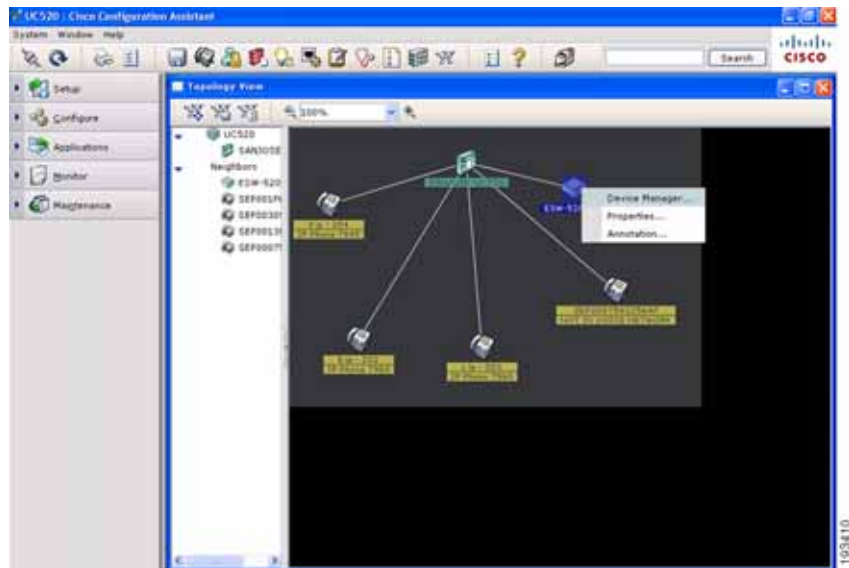
- Device Manager
- Properties
- Annotation

You can now continue with configuring the switch by two different options; use CCA to do all of the configuration, or use the Device Manager to go to the switch Configuration Utility. Additional information is described in detail in the appropriate [CCA user documentation](#). This procedure uses the Device Manager.

## Getting Started

### Connecting to the Switch

#### CCA Topology View page



**STEP 7** Click on **Device Manager**.

The *Log In* page will launch in a new browser window.

#### Log In page



**STEP 8** Enter a user name and password. The default user name is *cisco* and the default password is *cisco*. Passwords are both case sensitive and alpha-numeric.

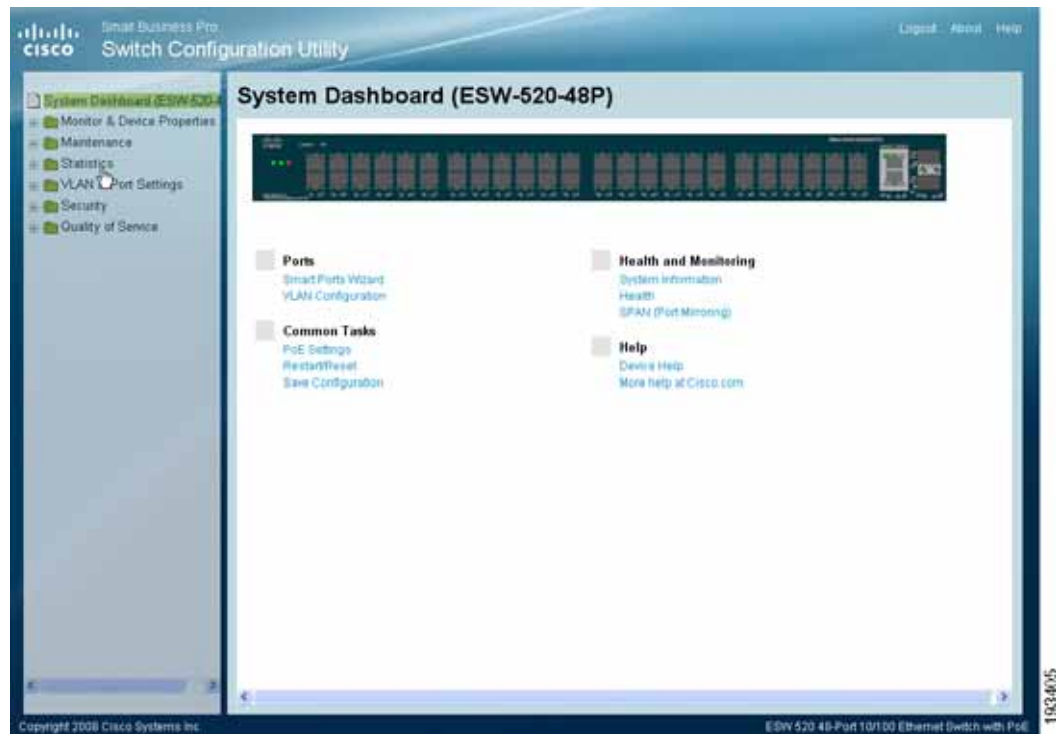
**STEP 9** Click **Log In**. The *Switch Configuration Utility - System Dashboard* Page opens.

## Getting Started

### Connecting to the Switch

**STEP 10** A window opens that prompts you to change your username and password from the default. Choose a new username and password, then click **Apply**.

### Switch Configuration Utility - System Dashboard

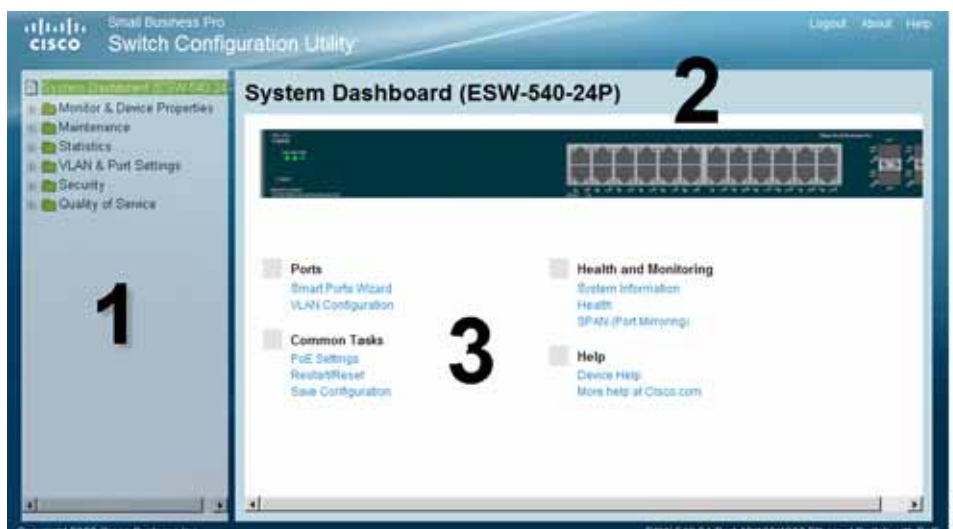


**STEP 11** You are now ready to proceed with additional switch configuration.

## Navigating The Cisco Switch Configuration Utility

The Cisco Switch Configuration Utility is a web-based device manager that is used to provision the switch. You must have IP connectivity between the PC and the switch to configure the switch. The following section describes how to navigate within the interface.

### Switch Configuration Utility - System Dashboard Page



The following table lists the interface components with their corresponding numbers:

Component	Description
<b>1</b> Navigation Pane	The navigation pane provides easy navigation through the configurable device features. The main branches expand to provide the subfeatures.
<b>2</b> Device View	The device view contains a graphical representation of the device faceplate, including the device status and port LEDs. Clicking on a port will open up the Edit Port Page.
<b>3</b> Getting Started Links	The getting started links allow you to navigate through the different device features.

### Using the Management Buttons

Device Management buttons and icons provide an easy method of configuring device information.

## Performing Common Configuration Tasks

Once the Switch Configuration Utility has been launched and you have logged into the switch, these are some examples of the common configuration tasks you can perform. Use the menus in the left navigation panel to choose a specific area of configuration.

### Checking the Software Version

To check the version of the software on the switch, click **About** at the top of the page.

#### Software Version Page



### Checking the System Information

Click on **Monitor & Device Properties > System Management > System Information**. The *System Information* page opens.

## Getting Started

### Performing Common Configuration Tasks

#### System Information Page

The screenshot shows the Cisco Small Business Pro Switch Configuration Utility interface. The left sidebar contains a tree view with the following items: System Dashboard (ESW-520-48P), Monitor & Device Properties, System Management, System Information (highlighted), Health, Restart / Reset, TCAM Utilization, Time, IP Addressing, Domain Name System (DNS), SNMP, CDP, Maintenance, Statistics, VLAN & Port Settings, Security, and Quality of Service. The main content area is titled 'System Information' and contains the following fields:

System Name	ESW-520-48P
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.9.1.1060
System Up Time	0 days, 3 hours, 9 minutes, 50 seconds
Base MAC Address	00:21:1b:1e:76:0a
Software Version	1.0.0.23
Boot Version	1.0.0.02

Below these fields is a 'Unique Device Identifier' section with a table:

PID	VID	SN
ESW-520-48P	V01	DN12450048

An 'Apply' button is located at the bottom of the form. The footer of the page includes 'Copyright 2008 Cisco Systems Inc.' and 'ESW 520 48-Port 10/100 Ethernet Switch with PoE'.

From this page you can configure the hostname of the switch, location and contact information for support. Also, you can view important information such as the system uptime, software version, MAC Address and Serial Number (SN).

#### Viewing what Devices are Attached to the Switch

To view what devices there are attached to the switch, click **Monitor & Device Properties > CDP**. The *CDP* page opens.

## CDP Page

System Dashboard (ESW-520-SP)

Monitor & Device Properties

- System Management
- SNMP
- CDP**
- Bonjour
- Maintenance
- Statistics
- VLAN & Port Settings
- Security
- Quality of Service

### CDP

CDP Status:

Voice VLAN:

#### Neighbors Table

Device ID	Local Interface	Advertised Version	Time to Live	Capabilities	Platform
<input type="radio"/> SP000E08D3A7DB	e5	2	165	H P	Linksys IP Phone SPA
<input type="radio"/> SP000E08D10ADB	e6	2	175	H P	Linksys IP Phone SPA
<input type="radio"/> SP000584D8C4BA	e7	2	145	H P	Cisco IP Phone SPA50
<input type="radio"/> SP000584D8BE02	e8	2	125	H P	Cisco IP Phone SPA50
<input type="radio"/> ESW-520-24P	g1	2	125	S I D	ESW-520-24P

© Copyright 2009 Cisco Systems Inc. ESW 520 8-Port 10/100 Ethernet Switch with PoE

Review the ports for connecting IP Phones, PCs, Access Points and the uplink to the Cisco UC520 or SR520. You can change the Voice VLAN from the default of 100 if required.

## Configuring the VLAN Settings for the Switch

To add or edit the default VLAN settings, click on **VLAN & Port Settings > VLAN Management > Properties**. The *Properties* page opens.



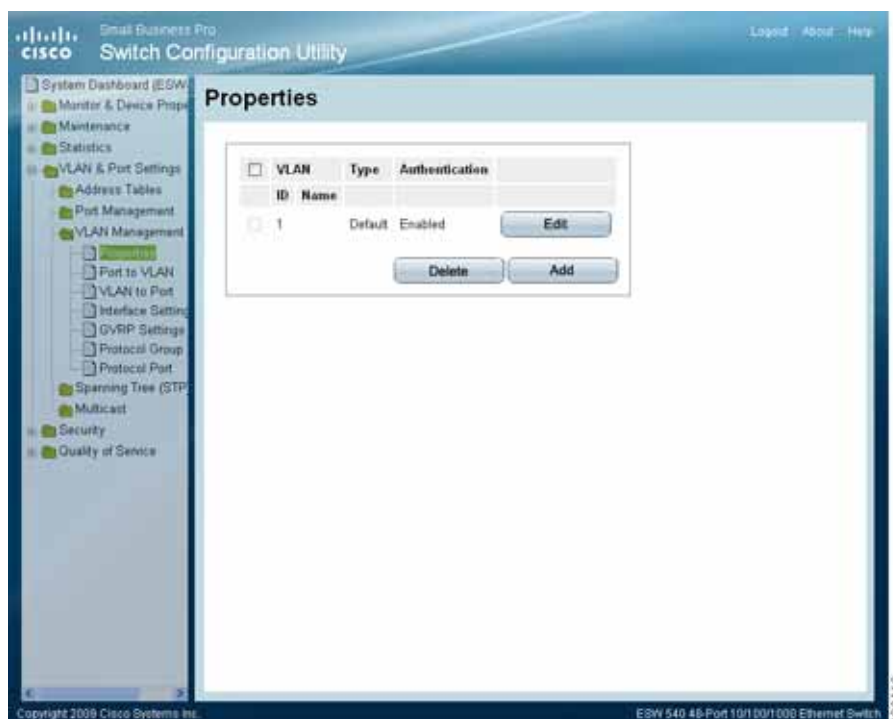
**NOTE** If the ESW 500 series switch is being deployed into a Cisco SBCS network, the installation is plug and play. If the switch is being deployed into a non-Cisco network, you will need to manually change VLAN settings.



## Getting Started

### Performing Common Configuration Tasks

#### Properties Page



#### Configuring individual ports using Cisco Smartport Roles

Smartport Roles make it easy to provision switch ports by automatically applying the appropriate configuration for attached IP phones, access points, or other devices to optimize network performance. The ESW 500 series switches support the predefined roles listed below:

Role	Description
Desktop	<ul style="list-style-type: none"><li>Optimized for desktop connectivity</li><li>Configurable VLAN setting</li><li>Port security enabled to limit unauthorized access to the network</li></ul>
IP Phone + Desktop	<ul style="list-style-type: none"><li>Optimized Quality of Service (QoS) for IP phone + desktop configurations</li><li>Voice traffic is placed on "Cisco-Voice" VLAN</li><li>Configurable data VLAN</li><li>QoS level assures voice-over-IP (VoIP) traffic takes precedence</li><li>Port security enabled to limit unauthorized access to the network</li></ul>

## Getting Started

### Performing Common Configuration Tasks

Role	Description
Router	<ul style="list-style-type: none"><li>Configured for optimal connection to a router or firewall for WAN connectivity</li></ul>
Switch	<ul style="list-style-type: none"><li>Configured as an uplink port to another switch or router Layer 2 port for fast convergence</li><li>Enables 802.1Q trunking</li></ul>
Access Point	<ul style="list-style-type: none"><li>Configured for optimal connection to a wireless access point</li><li>Configurable VLAN</li></ul>
Guest	<ul style="list-style-type: none"><li>Configured for a guest in a company, where the user would need to be restricted to specific applications.</li></ul>
Server	<ul style="list-style-type: none"><li>Configured for optimal connection to a server</li></ul>
Printer	<ul style="list-style-type: none"><li>Configured for optimal connection to a printer</li></ul>
VS Camera	<ul style="list-style-type: none"><li>Configured for optimal connection to a Video Surveillance Camera</li></ul>
Other	<ul style="list-style-type: none"><li>An "Other" Smartports role allows for flexible connectivity of non-specified devices</li><li>Configurable VLAN</li><li>No security</li><li>No QoS policy</li></ul>

## Smartport Roles

Default Smartport Roles applied to the individual ports for each type of device are as follows:

ESW 500 Series	Layer 2 Switch Ports		Uplink Ports
	Desktop Smartport Role	IP Phone + Desktop Smartport Role	Switch Smartport Role
ESW 520-8P	-	1-8	G1
ESW 540-8P	-	1-8	G1
ESW 520-24	1-24	-	G1-G4
ESW 520-24P	-	1-24	G1-G4
ESW 520-48	1-48	-	G1-G4
ESW 520-48P	-	1-48	G1-G4
ESW 540-24	1-10, 13-22	-	11-12, 23-24
ESW 540-24P	-	1-10, 13-22	11-12, 23-24
ESW 540-48	1-22, 25-46	-	23-24, 47-48



**NOTE** The G in the port tables denotes 10/100/1000 (Gigabit) copper or GBIC ports on the ESW520 series switches, and denotes the single G1 interface on the 8 port versions of the switch.

The following steps show one example of using the Smart Ports Setting Wizard to configure access points. It is not necessary to configure your switch in this manner.

**STEP 1** Click on the **System Dashboard**, and then on the **Smartports Wizard**. The *Smart Ports Wizard* opens.

To change a port from the default setting to a different role, highlight the appropriate port on this page by clicking on it, then select a different profile from the drop-down list under Assign Profile:

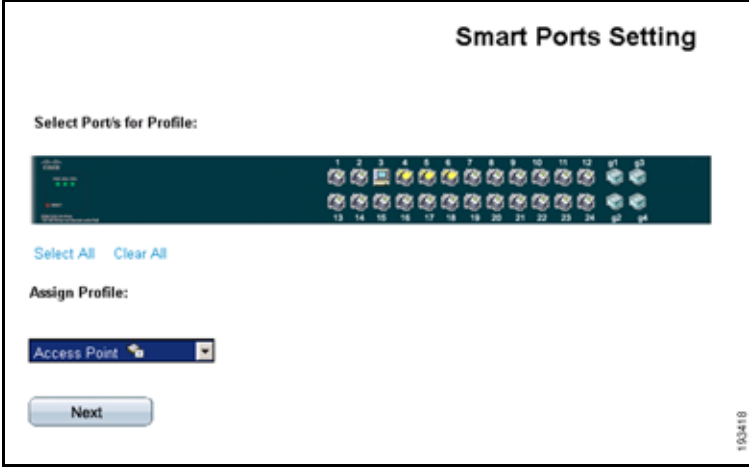
#### Smart Ports Setting Wizard

**STEP 2** Configure ports 4-6 for Access Points.

## Getting Started

### Performing Common Configuration Tasks

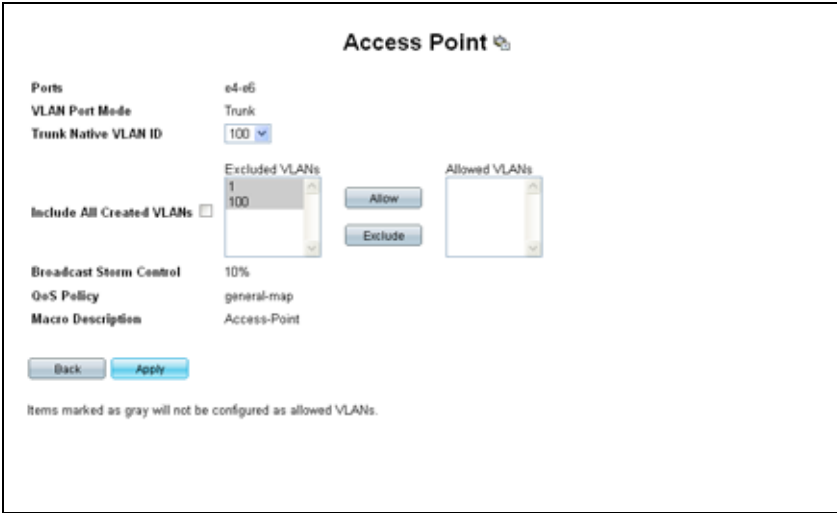
#### Smart Ports Setting Wizard



The screenshot shows the 'Smart Ports Setting' window. At the top, it says 'Select Port's for Profile:'. Below this is a grid of 24 port icons arranged in two rows of 12. The first row is labeled 1 through 12, and the second row is labeled 13 through 24. Below the grid are two buttons: 'Select All' and 'Clear All'. Underneath is the 'Assign Profile:' section with a dropdown menu currently set to 'Access Point'. At the bottom is a 'Next' button. A small vertical text '100418' is visible on the right side of the window.

- STEP 3** Click **Next**. The *Access Point* window opens. To ensure all VLANs in the network are trunked to the Wireless Access Points, select the drop-down list beside **Trunk Allowed VLANs**. Select **vlan 100** from the drop-down list to allow voice over wireless.

#### Smart Ports Settings Wizard - Access Point



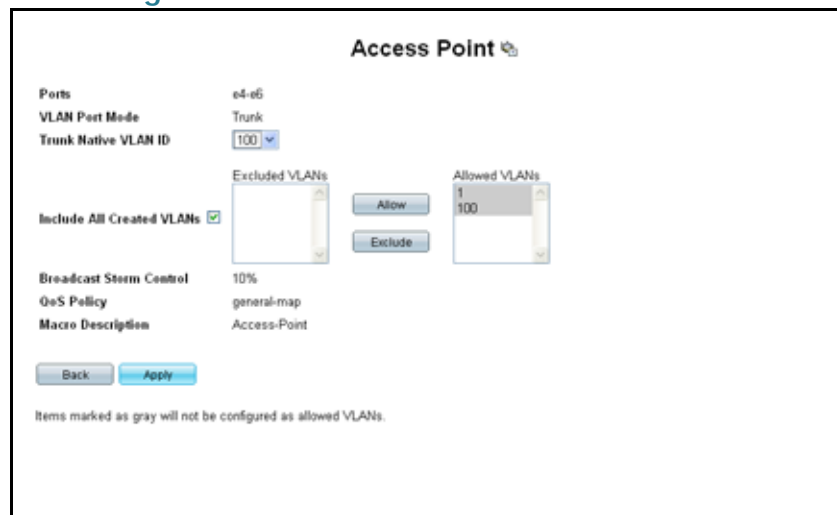
The screenshot shows the 'Access Point' configuration window. It has several sections: 'Ports' with a value of 'e4-e6'; 'VLAN Port Mode' set to 'Trunk'; 'Trunk Native VLAN ID' with a dropdown set to '100'; 'Include All Created VLANs' with an unchecked checkbox; 'Broadcast Storm Control' set to '10%'; 'QoS Policy' set to 'general-map'; and 'Macro Description' set to 'Access-Point'. There are two lists: 'Excluded VLANs' containing '1' and '100', and 'Allowed VLANs' which is empty. Between these lists are 'Allow' and 'Exclude' buttons. At the bottom are 'Back' and 'Apply' buttons. A note at the very bottom states: 'Items marked as gray will not be configured as allowed VLANs.'

- STEP 4** Click **Allow** to ensure that VLAN100 shows up in the allowed list, and then click **Apply**.

## Getting Started

### Performing Common Configuration Tasks

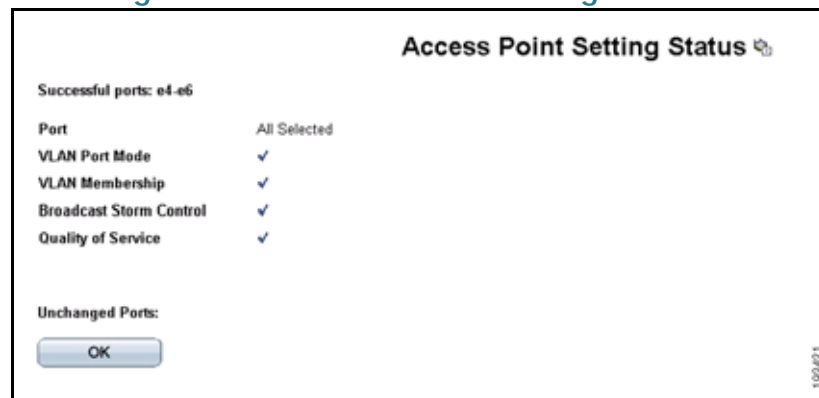
#### Smart Ports Settings Wizard - Access Point



The screenshot shows the 'Access Point' configuration window. It includes fields for 'Ports' (e4-e6), 'VLAN Port Mode' (Trunk), and 'Trunk Native VLAN ID' (100). There are two lists: 'Excluded VLANs' and 'Allowed VLANs'. The 'Allowed VLANs' list contains '1' and '100'. Below these lists are 'Allow' and 'Exclude' buttons. Other settings include 'Include All Created VLANs' (checked), 'Broadcast Storm Control' (10%), 'QoS Policy' (general-map), and 'Macro Description' (Access-Point). At the bottom are 'Back' and 'Apply' buttons. A note at the bottom states: 'Items marked as gray will not be configured as allowed VLANs.'

**STEP 5** A confirmation page opens. Review your changes and click **OK**.

#### Smart Ports Settings Wizard - Access Point Setting Status



The screenshot shows the 'Access Point Setting Status' confirmation window. It lists 'Successful ports: e4-e6' and a table of settings:

Port	Setting
VLAN Port Mode	All Selected
VLAN Membership	✓
Broadcast Storm Control	✓
Quality of Service	✓

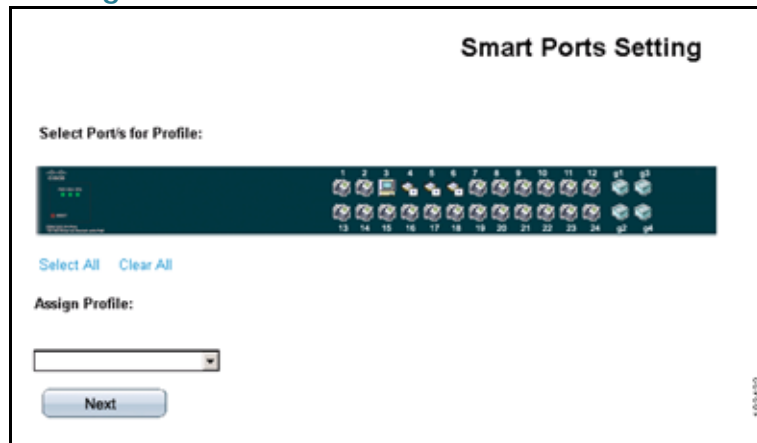
Below the table is the 'Unchanged Ports:' section and an 'OK' button. A small vertical text '10/24/11' is on the right side.

**STEP 6** Return to the System Dashboard and click on the **Smart Ports Wizard**. The icons for ports 4-6 should appear as follows:

## Getting Started

### Performing Common Configuration Tasks

#### Smart Ports Setting



The image shows a 'Smart Ports Setting' configuration window. At the top, it says 'Smart Ports Setting'. Below that, it says 'Select Port/s for Profile:'. There is a grid of 24 port icons, numbered 1 through 24. Below the grid, there are two buttons: 'Select All' and 'Clear All'. Below that, it says 'Assign Profile:'. There is a dropdown menu for selecting a profile. At the bottom, there is a 'Next' button. On the right side of the window, there is a vertical label '193422'.

#### Checking the Device Power Consumption

Check the overview of the power consumption on the switch. Click **System Dashboard > PoE Settings**. The *PoE Settings* page opens.

## PoE Settings Page

**PoE Settings**

Total PoE Power Consumption (W) 0

Total PoE Power Available (W) 290

Port	Admin Status	Priority	Power Allocation (mW)	Power Consumption (mW)	
g1	Enable	Low	15400	0	Edit
g2	Enable	Low	15400	0	Edit
g3	Enable	Low	15400	0	Edit
g4	Enable	Low	15400	0	Edit
g5	Enable	Low	15400	0	Edit
g6	Enable	Low	15400	0	Edit
g7	Enable	Low	15400	8600	Edit
g8	Enable	Low	15400	0	Edit
g9	Enable	Low	15400	0	Edit
g10	Enable	Low	15400	0	Edit
g11	Enable	Low	15400	0	Edit
g12	Enable	Low	15400	0	Edit
g13	Enable	Low	15400	0	Edit
g14	Enable	Low	15400	0	Edit
g15	Enable	Low	15400	0	Edit

Copyright 2008 Cisco Systems Inc. ESW 540 24-Port 10/100/1000 Ethernet Switch with PoE

Click **Edit** to change a PoE setting.

The number of PoE devices supported on a switch depends on the power requirements for each device and the switch model in question. To help illustrate this, the PoE Device Support table shows the recommended number of POE devices for 3 different scenarios:

**Scenario 1** — Assumes the POE devices connected to the switch are all IEEE 802.3af Class 2 devices which draw less than 7.5W per device

**Scenario 2** — Assumes the POE devices connected to the switch are a mix of IEEE 802.3af Class 2 & Class 3 devices which on average draw less than 11W per device

**Scenario 3** — Assumes the POE devices connected to the switch are all IEEE 802.3af Class 3 devices which draw less than 15.4W per device

## Getting Started

### Performing Common Configuration Tasks

#### PoE Device Support

ESW 500 Series Switch	Total Power	Scenario 1 PoE Devices drawing < 7W	Scenario 2 PoE Devices drawing < 11W	Scenario 3 PoE Devices drawing < 15.4 W
ESW 520-8P	60 Watts	Up to 15.4 Watts to each port up to the total budget		
ESW 540-8P	120 Watts	Up to 15.4 Watts to each port up to the total budget		
ESW 520-24P	180 Watts	24 Devices	16 Devices	12 Devices
ESW 520-48P	380 Watts	48 Devices	32 Devices	24 Devices
ESW 540-24P	280 Watts	24 Devices	24 Devices	18 Devices

In these scenarios, a device would be a wireless access point, IP phone, video surveillance camera or other such device. Refer to the information that came with your specific device for power consumption information.

Refer to additional sections in this guide for details on further PoE configuration.

#### Saving the Configuration

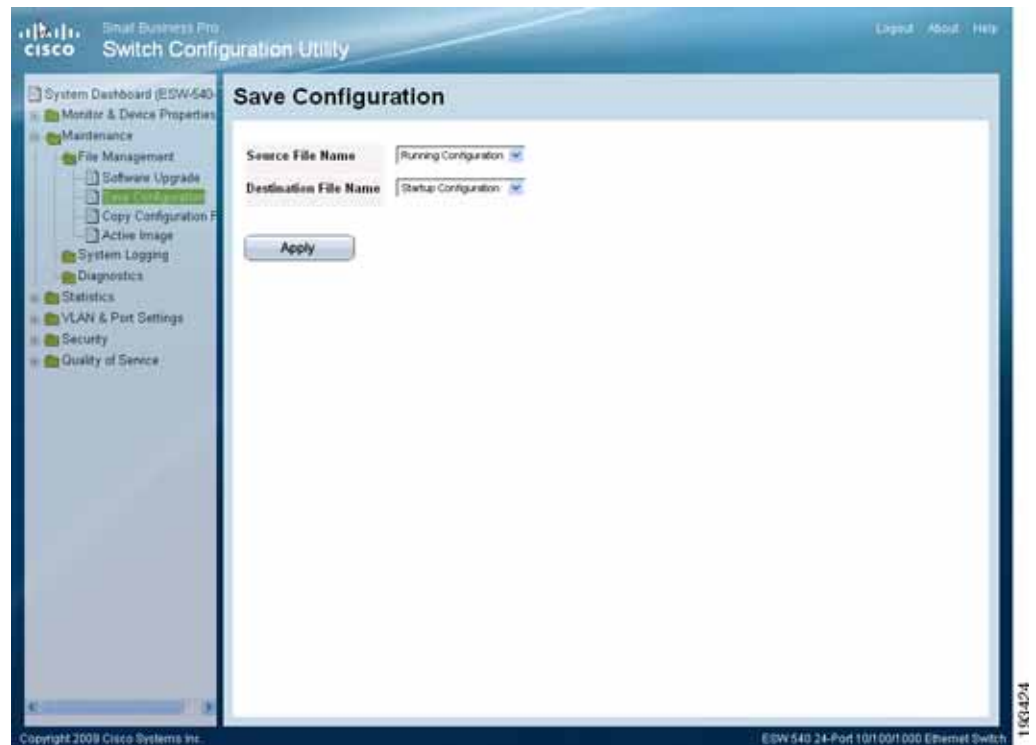
After any changes, always make sure to save the switch configuration. Click **Maintenance > File management > Save Configuration**. The *Save Configuration* page opens.



## Getting Started

### Performing Common Configuration Tasks

#### Save Configuration Page



The *Save Configuration* Page contains the following fields:

**Source File Name** — Indicates the device configuration file to copy and the intended usage of the copied file (Running, Startup, or Backup).

**Destination File Name** — Indicates the device configuration file to copy to and the intended usage of the file (Running, Startup, or Backup).

Define the relevant fields and then Click **Apply**. The Configuration Files are updated.

Another option to quickly save the Running Configuration to the Startup Configuration is to click **Save Configuration** at the top of the page. This link is initially grayed out. Once switch configuration changes are made, the link becomes active.

#### Upgrading the Firmware on the Switch


The following steps show how to download, install, and make a new firmware release the active image on the switch.

## Getting Started

### Performing Common Configuration Tasks

- STEP 1** Ensure the PC has IP connectivity to the ESW 500 series switch.
- STEP 2** The switch can be upgraded through the TFTP or HTTP protocol. If you choose to use TFTP, the PC needs to have a TFTP server running on it. A free TFTP server can be downloaded from:
- <http://www.solarwinds.com/downloads/index.aspx>
- STEP 3** Download the latest ESW 500 series software file from:
- [www.cisco.com/go/esw500help](http://www.cisco.com/go/esw500help)
- If you choose to use TFTP, make sure it is stored in the root directory of the TFTP server running on your PC.
- STEP 4** Download the software image from the PC to the ESW 500 series switch. Click on **Maintenance > File Management > Software Upgrade**. The *Software Upgrade* page opens.

#### Software Upgrade Page

The screenshot shows the Cisco Switch Configuration Utility interface. On the left is a navigation pane with a tree structure. The 'Software Upgrade' option under 'File Management' is highlighted. The main content area is titled 'Software Upgrade' and contains two radio buttons: 'UPGRADE' (selected) and 'BACKUP'. Below these are two input fields: 'via TFTP' (selected) and 'via HTTP'. Further down are three input fields: 'File Type' (set to 'Software Image'), 'TFTP Server', and 'Source File'. An 'Apply' button is at the bottom of the form. The footer of the page includes the copyright notice '© Copyright 2009 Cisco Systems, Inc.' and the device model 'ESW 520 24-Port 10/100 Ethernet Switch with PoE'.

- STEP 5** For TFTP: Enter the PC IP address in the *TFTP Server* field, the exact filename for the image in *Source File* field, then click **Apply**. The *Software Upgrade* page shows the progress of the download.

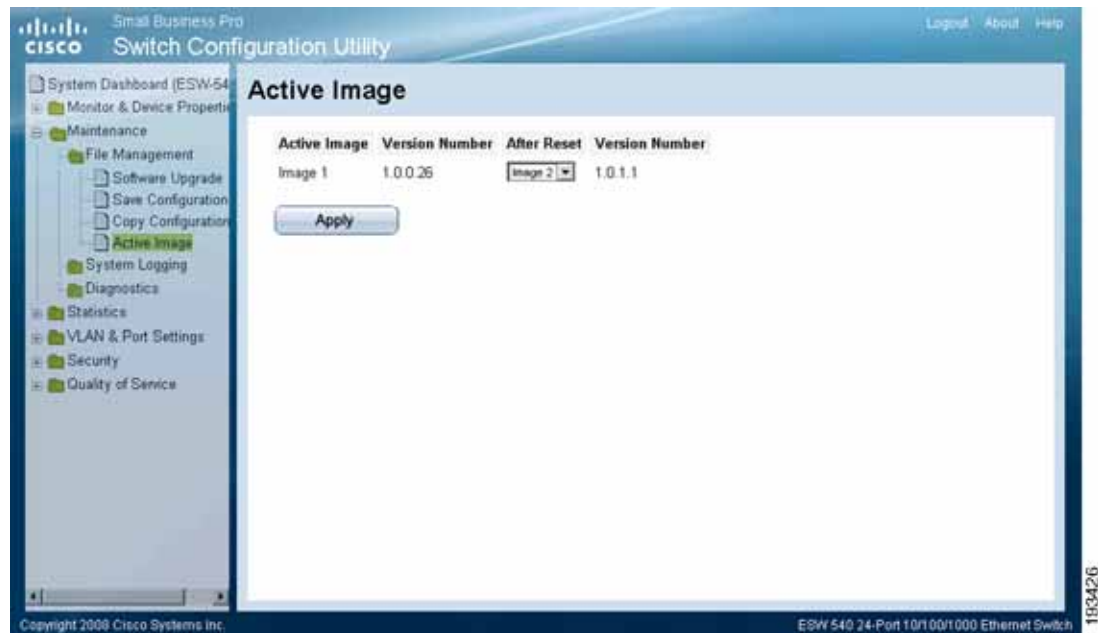
## Getting Started

### Performing Common Configuration Tasks

For HTTP: Click **Browse** and navigate to the file name of the image.

- STEP 6** Once the download is complete, click on **Maintenance > File Management > Active Image**. The *Active Image* page opens.

#### Active Image Page



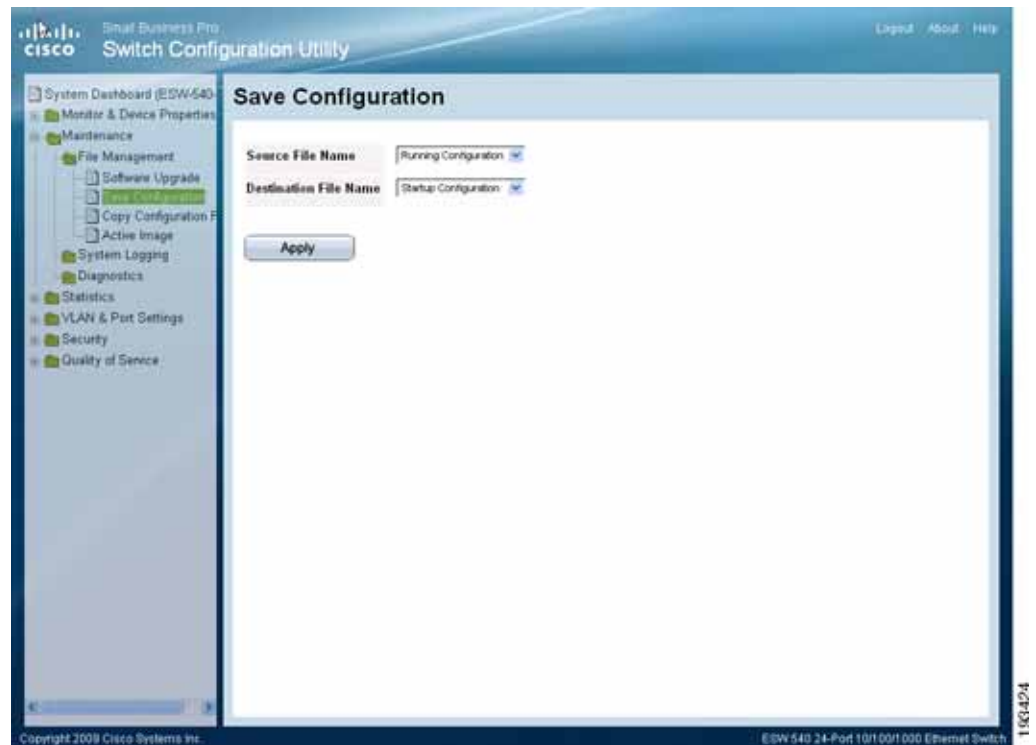
- STEP 7** Choose the new image from the drop-down list under *After Reset* and click **Apply**.

- STEP 8** Save the switch configuration. Click **Maintenance > File Management > Save Configuration**. The *Save Configuration* page opens.

## Getting Started

### Performing Common Configuration Tasks

#### Save Configuration Page



**STEP 9** Keep the defaults for *Source File Name* and *Destination File Name* and click **Apply**.

**STEP 10** Reset the switch by clicking on **Monitor & Device Properties > System Management > Restart / Reset**.

## Getting Started

### Performing Common Configuration Tasks

#### Restart / Reset Page



**STEP 11** Click on **Reset / Reboot** and the switch should reboot with the new image.

**STEP 12** After the switch has completed rebooting and is up and running, log back in.

**STEP 13** Ensure the software has been upgraded by clicking on **About** at the top of the Dashboard page. A version page will appear:



## Resetting the Device

The Restart / Reset Page enables the device to be reset from a remote location. Save all changes to the Running Configuration file before resetting the device by clicking on **Maintenance > File Management > Save Configuration**. Define the relevant fields and then click **Apply**. This prevents losing the current device configuration.

To reset the device:

- STEP 1** Click **Monitor & Device Properties > System Management > Restart / Reset**. The Restart / Reset Page opens.

### Restart / Reset Page



- STEP 2** Click one of the available Reset commands:
- **Reset / Reboot** — Resets the device. Ensure the device configuration has been saved.
  - **Restore Default** — Restores the device to the factory default configuration.
- STEP 3** After the switch has completed rebooting and is up and running, relaunch the Switch Configuration Utility and log back into the switch.

## Getting Started

### Performing Common Configuration Tasks

---



---

**NOTE** If using CCA to launch the Switch Configuration Utility, **right-click** on switch > Device Manager. Refresh the topology screen to get the latest IP address for the switch.

---

### Manual Reset

The Switch can be reset by inserting a pin or paper clip into the RESET opening. Pressing the manual reset for 0 to 10 seconds reboots the switch. Pressing the manual reset for longer than 10 seconds results in the switch being reset to factory defaults.

### Logging Off the Device

Click **Logout** at the top of the page. The system logs off. The *Switch Configuration Utility* closes and the Log In page opens.

## Using The Switch Console Port

The switch features a menu-based console interface for basic configuration of the switch and management of your network. The switch can be configured using the menu-based interface through the console port or through a telnet connection. This section describes console interface configuration.



#### TIP

Configuration of the switch through the Console Port requires advanced skills. This should only be attempted by trained personnel.

### Selecting Menu Options and Actions

Within the Console Interface, menus list options in numeric order. Actions appear at the end of the page. To select menu options and actions, use the following keys on your keyboard:

Key	Function
Arrow keys	Move the cursor up, down, left, or right.
Number key	Press the menu number and then press Enter key to select a menu option.
Tab	Move the cursor from one field to the next on an editing page.
Enter	Select an option that is highlighted by the cursor.
Esc	Return to the previous menu or page, or move cursor from editable fields to <i>Action</i> list.

Use the following steps to connect to the switch using the console:

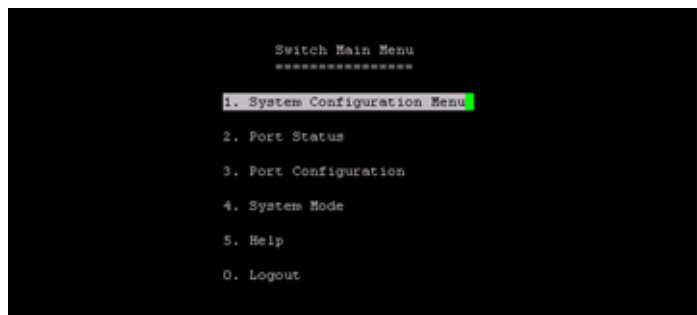
- STEP 1** Power up the ESW 500 Series switch.
- STEP 2** Connect it to the network if required.
- STEP 3** Use the console cable supplied with the switch to connect the serial port on the PC to the console port on the switch.



## Getting Started

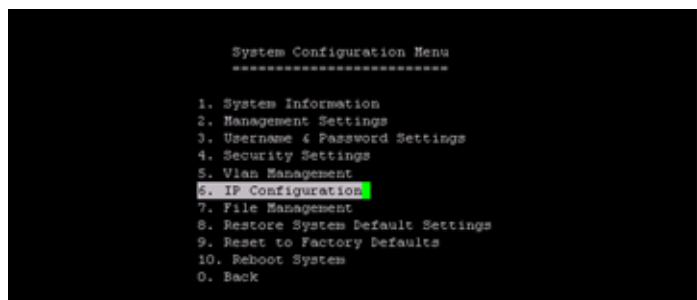
### Using The Switch Console Port

- STEP 4** On the PC, launch a terminal emulation program such as HyperTerminal (bundled with Windows) or Putty (freeware) and configure a new connection with the following settings:
- Speed or Bits Per Second — 115200
  - Data Bits — 8
  - Stop Bit — 1
  - Parity — None
  - Flow Control — None
  - Serial Port — Choose the appropriate serial or COM port on the PC that the console cable is connected to
- STEP 5** Save these settings and open a connection using the terminal emulation software. If a blinking cursor appears, press **Tab** and enter the default username *cisco* and press **Tab** again and enter the default password *cisco*. Press **Enter** to continue.
- STEP 6** The switch main menu opens.



The System Configuration Menu line should be highlighted.

- STEP 7** Press **Enter**. The page changes to System Configuration Menu.



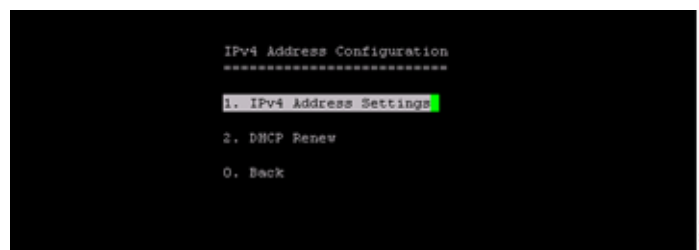
## Getting Started

### Using The Switch Console Port

- STEP 8** Scroll down to option 6, IP Configuration, and press **Enter**. The IP Configuration Menu opens.



- STEP 9** Highlight option 1, IPv4 Address Configuration, and press **Enter**. The IPv4 Address Configuration Menu opens.



- STEP 10** Highlight option 1, IPv4 Address Settings, and press **Enter**. The IPv4 Address Settings page opens.



## Getting Started

### Using The Switch Console Port

The current IP address setting for the ESW 500 series switch is shown. If the switch is already connected to the network and obtained an IP address via DHCP, this is the IP address which is used to launch the ESW 500 Switch Configuration Utility.

If you need to change the IP address to a static IP address, perform the following steps:

- STEP 1** Use the Right arrow key to highlight Edit, then press **Enter**. The IPv4 Address field should be highlighted.
- STEP 2** Using the arrow keys to navigate around the window, and the enter key to apply changes, modify the IPv4 Address, Subnet mask, and Default Gateway.
- STEP 3** Change the DHCP Client field to be Disable by pressing the **space bar**.
- STEP 4** Press the **ESC** key, press the **right arrow** to highlight Save, and press **Enter** to save all changes.

# Managing Device Information

This section provides information for defining both basic and advanced system information. This section contains the following topics:

- Understanding the Dashboards
- Defining System Information
- Viewing Device Health
- Managing Cisco Discovery Protocol
- Defining the Bonjour Discovery Protocol
- TCAM Utilization

## Understanding the Dashboards

The *System Dashboard* page is the main window and contains links for configuring ports, viewing device health information, common device tasks, and viewing online help.

- **Ports** — Includes Smartports Wizard and VLAN Configuration
- **Health and Monitoring** — Includes System Information, Health, and SPAN (Port Mirroring)
- **Common Tasks** — Includes PoE Settings (PoE switches only), Restart/Reset, and Save Configuration
- **Help** — Includes online Device Help and More help at Cisco.com

To open the *System Dashboard* Page:

Click **System Dashboard** (*Device Name*). The System Dashboard page for your device opens:

## Managing Device Information

### Understanding the Dashboards

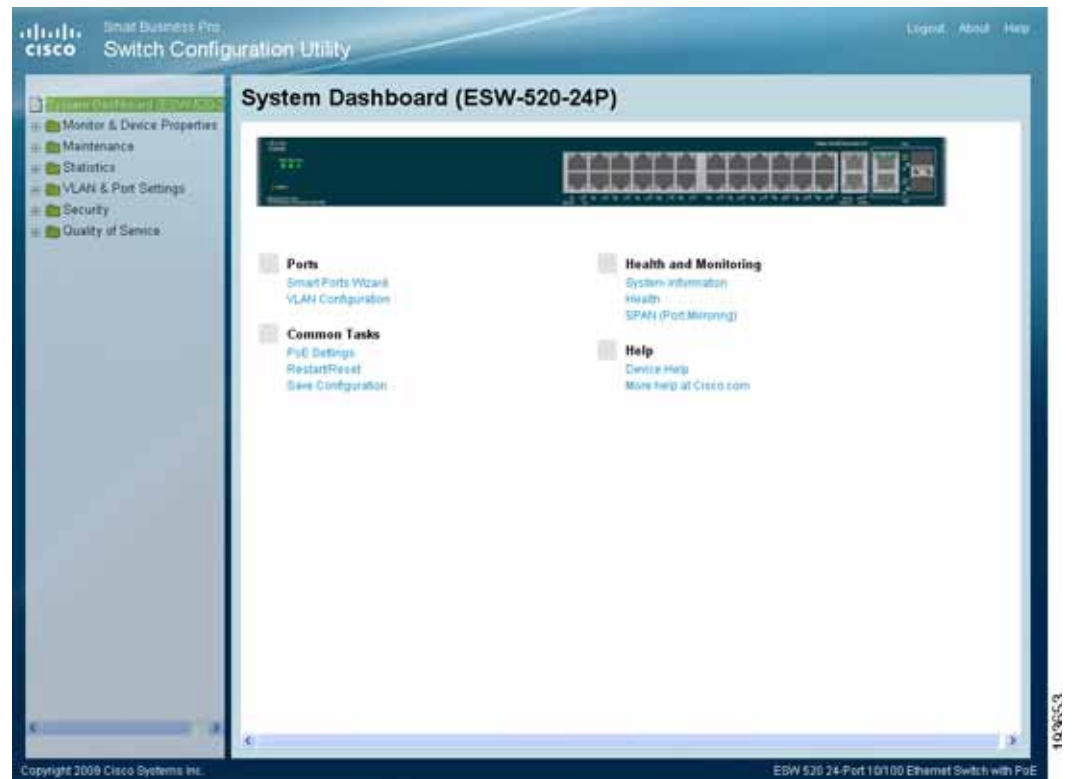
#### System Dashboard (ESW-520-24) Page



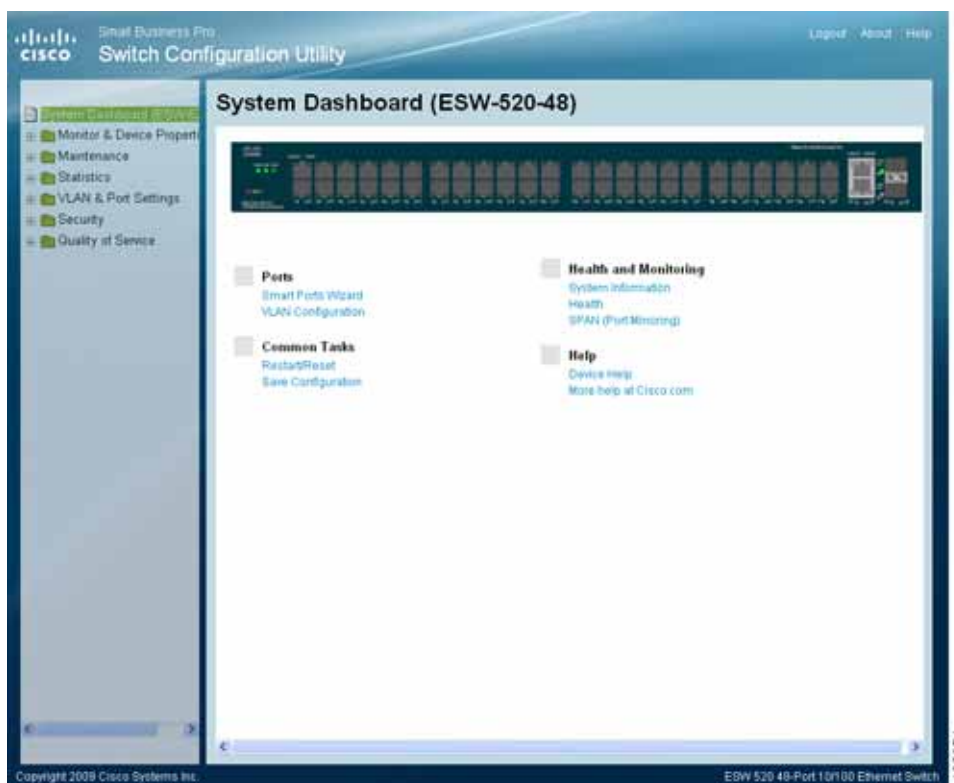
## Managing Device Information

### Understanding the Dashboards

#### System Dashboard (ESW-520-24P) Page



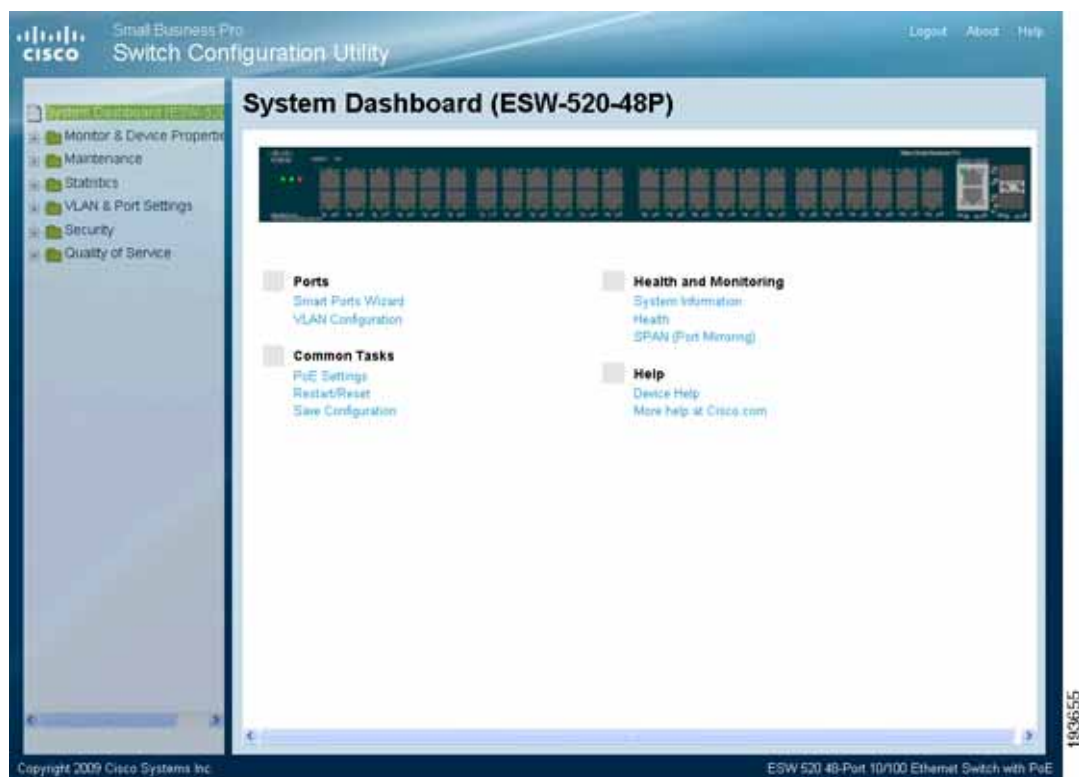
#### System Dashboard (ESW-520-48) Page



## Managing Device Information

### Understanding the Dashboards

#### System Dashboard (ESW-520-48P) Page

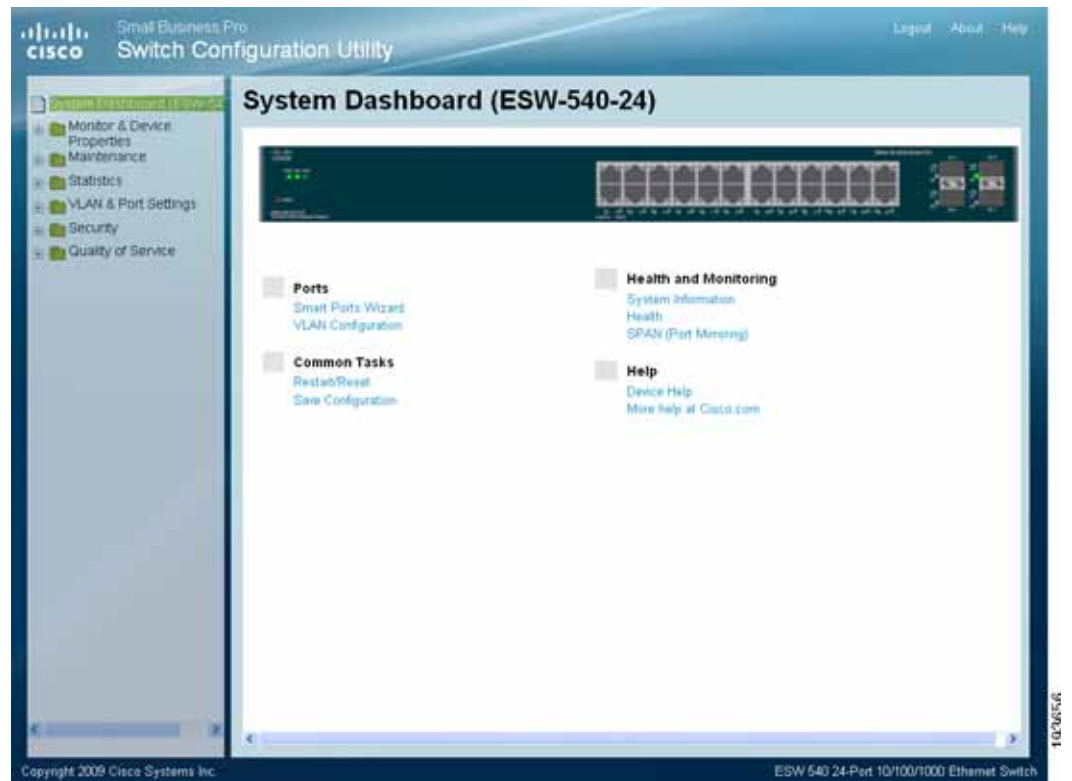




## Managing Device Information

### Understanding the Dashboards

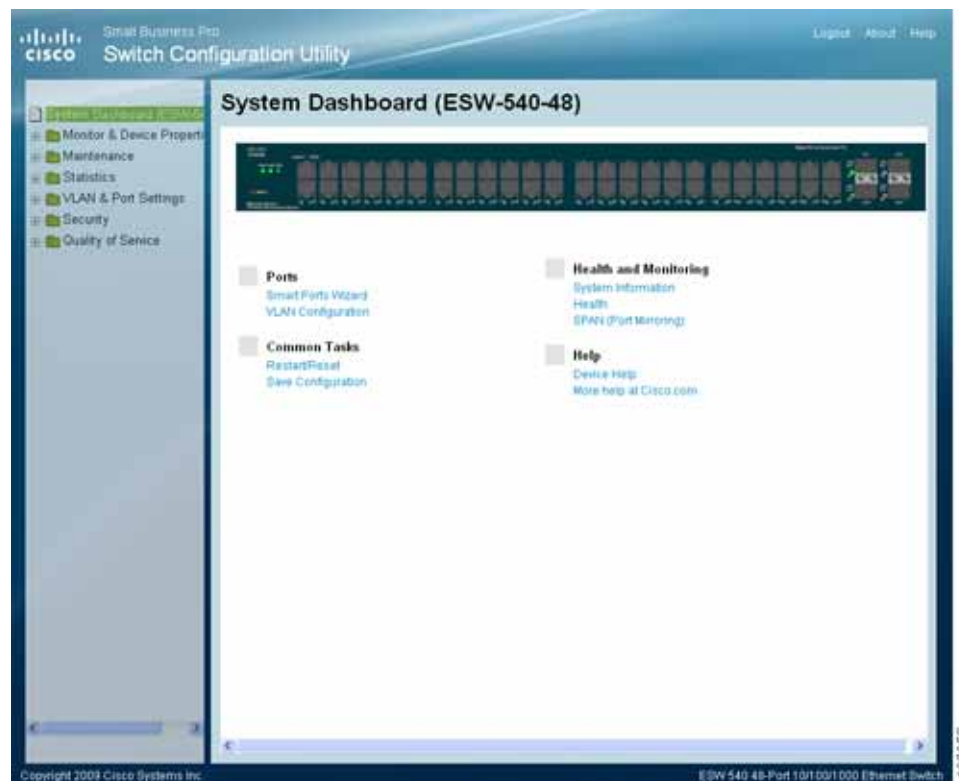
#### System Dashboard (ESW-540-24) Page



#### System Dashboard (ESW-540-24P) Page



#### System Dashboard (ESW-540-48) Page



You can edit a specific port on the switch by clicking on that port from the device view.

The *System Dashboard* page contains the following port indicators in the device graphical representation:

- **Green** — Indicates the port is currently operating.

The *System Dashboard* pages contains the links to the following:

#### Ports

- **Smart Ports Wizard** — Opens the Smart Ports Wizard page.
- **VLAN Configuration** — Opens the VLAN Properties Page.

#### Health and Monitoring

- **System Information** — Opens the System Information Page.
- **Health** — Opens the Health Page.
- **SPAN (Port Mirroring)** — Opens the SPAN (Port Mirroring) Page.

#### Common Tasks

- **PoE Settings** — Opens the PoE Settings Page (PoE switches only)
- **Restart / Reset** — Opens the Restart/Reset Page.
- **Save Configuration** — Opens the Save Configuration Page.

#### Help

- **Device Help** — Opens the online help.
- **More help at Cisco.com** — Provides a link to online Technical Support.

## Defining System Information

The *System Information Page* contains parameters for configuring general device information. To open the *System Information Page*:

- STEP 1** Click **Monitor & Device Properties > System Management > System Information**. The *System Information Page* opens:

#### System Information Page

The screenshot shows the Cisco Switch Configuration Utility interface. On the left is a navigation tree with categories like System Dashboard, Monitor & Device Properties, System Management, Health, Restart / Reset, TCAM Utilization, Time, IP Addressing, Domain Name System (DNS), SNMP, CDP, Maintenance, Statistics, VLAN & Port Settings, Security, and Quality of Service. The 'System Management' category is expanded, and 'System Information' is selected. The main panel displays the 'System Information' configuration page. It includes fields for System Name (ESW-520-24), System Location, System Contact, System Object ID (1.3.6.1.4.1.9.1.1001), System Up Time (0 days, 2 hours, 23 minutes, 26 seconds), Base MAC Address (00:16:b6:01:73:70), Software Version (1.0.1.7), and Boot Version (1.0.0.02). Below these is a 'Unique Device Identifier' table with columns for PID, VID, and SN, containing the values ESW-520-24, V01, and 7NC006800221. An 'Apply' button is at the bottom.

PID	VID	SN
ESW-520-24	V01	7NC006800221

The *System Information Page* contains the following fields:

- **System Name** — Displays the user configured name of the system.
- **System Location** — Defines the location where the system is currently running. The field range is from 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is 0-160 characters.
- **Login Banner** — Defines a user-configurable message of up to 1000 characters
- **System Object ID** — Displays the vendor's authoritative identification of the network management subsystem contained in the entity.
- **System Up Time** — Displays the amount of time that has elapsed since the last device reset. The system time is displayed in the following format: Days, Hours,

Minutes and Seconds. For example: 41 days, 2 hours, 22 minutes and 15 seconds.

- **Base MAC Address** — Displays the device MAC address.
- **Software Version** — Displays the software version number.
- **Boot Version** — Indicates the system boot version currently running on the device.
- **Jumbo Frame** — Indicates if Jumbo Frames are enabled . Jumbo Frames become active after resetting the device. (Jumbo Frames are not available on ESW-520 devices). The possible field values are:
  - *Enable* — Enables Jumbo Frames on the device.
  - *Disable* — Disables Jumbo Frames on the device.
- **Unique Device Identifier** — Displays the Unique Device Identifier (UDI). The UDI provides a unique identifier for Cisco devices. The device comes with the UDI preconfigured. The UDI is composed of three parts, including:
  - **PID** — The Product Identifier (PID) is an alphanumeric identifier that identifies the specific Cisco hardware.
  - **VID** —The Version Identifier (VID) provides tracking for the Customer-Orderable PID version. The VD indicates the number reportable customer versions.
  - **SN** — The Serial Number (SN) is unique to device, and identifies the device and the Field Replaceable Unit (FRU).

**STEP 2** Define the relevant fields.

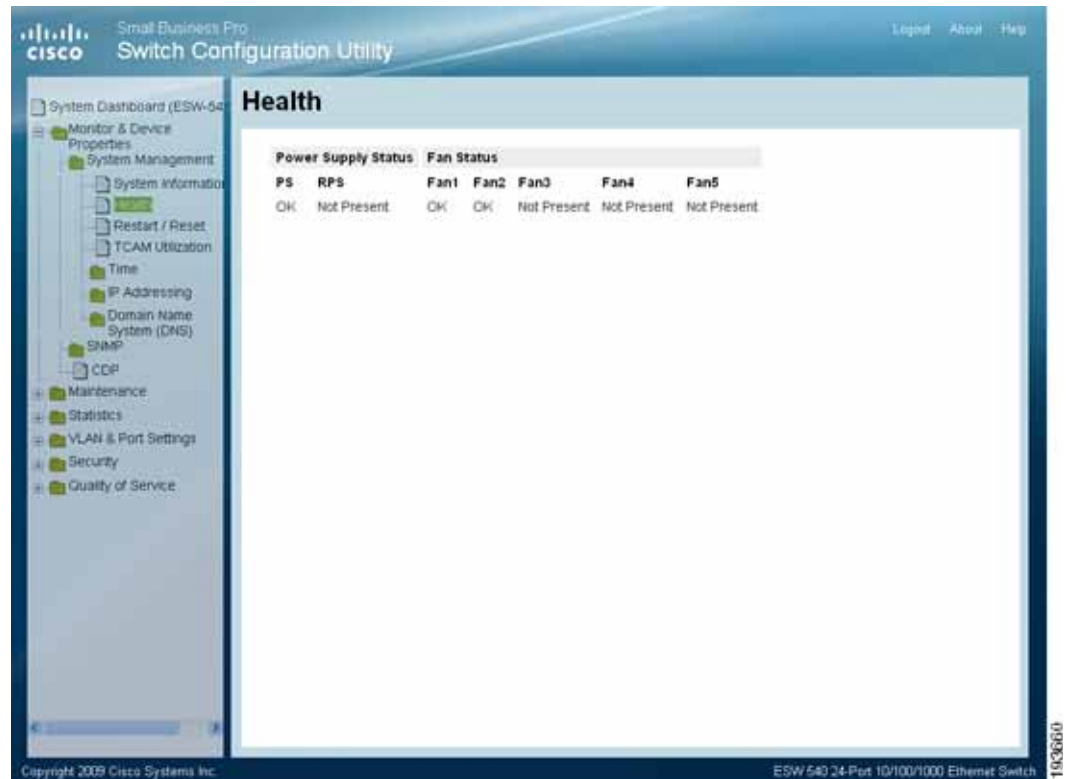
**STEP 3** Click **Apply**. The system information is defined, and the device is updated.

## Viewing Device Health

The *Health Page* displays physical device information, including information about the device's power and ventilation sources.

- STEP 1** Click **Monitor & Device Properties > System Management > Health**. The *Health Page* opens:

#### Health Page



The *Health Page* contains the following fields:

- **Power Supply Status** — Displays the power supply status. Power supply 1 is displayed as PS in the interface, while the redundant power supply is displayed as RPS. The possible field values are:
  - *OK* — Indicates the power supply is operating normally.
  - *Fail* — Indicates the power supply is not operating normally.
  - *Not Present* — Indicates a redundant power supply is not connected.
- **Fan Status** — Displays the fan status. The device has five fans. Each fan is denoted as fan plus the fan number. The possible field values are:
  - *OK* — Indicates the fan is operating normally.
  - *Fail* — Indicates the fan is not operating normally.

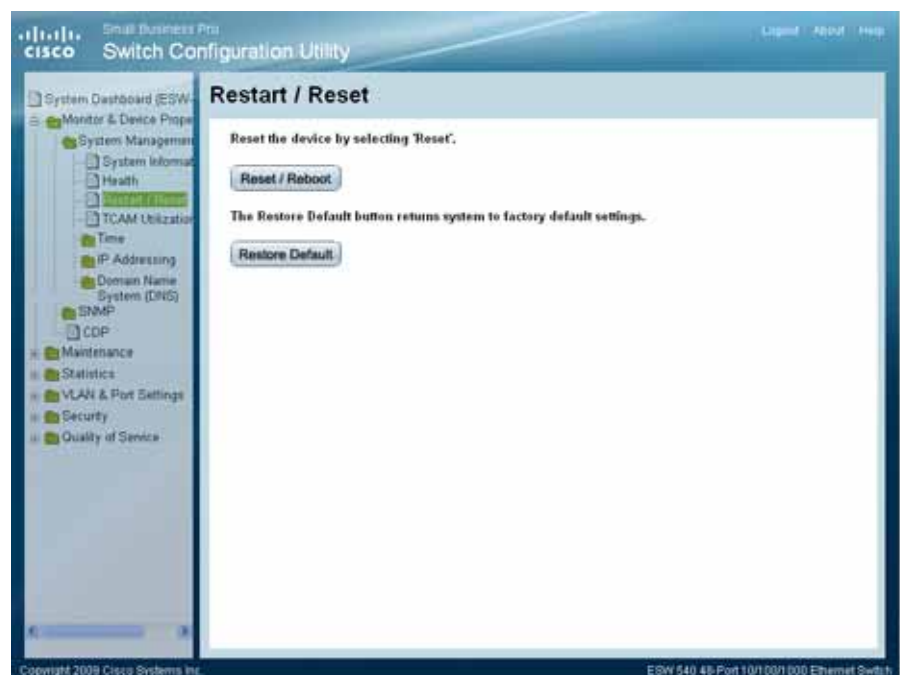
- *Not Present* -- Indicates the fan is not present.

## Resetting the Device

The *Restart / Reset* page enables the device to be reset from a remote location. Save all changes to the Running Configuration file before resetting the device. This prevents the current device configuration from being lost. To open the *Restart / Reset Page*:

- STEP 1** Click **Monitor & Device Properties > System Management > Restart / Reset**. The *Restart / Reset Page* opens:

### Restart / Reset Page



The following resets the device:

- **Reset / Reboot** — Resets the device. Ensure the device configuration has been saved.
- **Restore Default** — The device is restored to the factory default configuration.



## Managing Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol that enables devices to advertise their existence to other devices by CDP sending out periodic updates to a Multicast address. In addition, CDP allows devices to receive information about other devices on the same LAN or on the remote WAN side. The system supports CDP versions 1 and 2. To enable CDP on the device:

**STEP 1** Click **Monitor & Device Properties > CDP**. The *CDP Page* opens:

### CDP Page

Device ID	Local Interface	Advertise Version	Time to Live	Capabilities	Platform
SP000E0803A7D8	e5	2	165	H P	Linksys IP Phone SPA
SP000E08D10ADB	e6	2	175	H P	Linksys IP Phone SPA
SP000584D8C4BA	e7	2	145	H P	Cisco IP Phone SPA50
SP000584D8BE02	e8	2	125	H P	Cisco IP Phone SPA50
ESW-520-24P	g1	2	125	S I D	ESW-520-24P

The *CDP Page* contains the following fields:

The following fields are configurable by the user:

- **CDP Status** — Indicates if CDP is enabled on the device. The possible field values are:
  - *Enable* — Enables CDP on the device. This is the default value.
  - *Disable* — Disables CDP on the device.

- **Voice VLAN** — The Voice VLAN field displays the current Voice VLAN used by the switch. The default is VLAN #100. This VLAN carries the voice traffic, and is also advertised through the CDP to the other elements in the network. The user can change the Voice VLAN via this screen.

The following fields display Neighbors Information and are Read-only.

- **Device ID** — Indicates the device ID that is advertised by neighboring devices.
- **Local Interface** — Indicates the receiving port number.
- **Advertise Version** — Indicates the CDP version advertised by the neighboring device.
- **Time to Live** — Indicates the amount of time in seconds before the neighboring device CDP information is aged out. The field default is 180 seconds.
- **Capabilities** — Indicates the device capabilities advertised by the neighboring devices. There are 11 capabilities whereby each capability is represented by a one letter code. A neighbor device can advertise more than one capability, which is presented as a series of one letter codes, for example: S I D - represents Switch + Remotely-Managed-Device. The list of capabilities follows:
  - *R* — Router
  - *T* — Trans Bridge
  - *B* — Source Route Bridge
  - *S* — Switch
  - *H* — Host
  - *I* — IGMP
  - *r* — Repeater
  - *P* — VoIP-Phone
  - *D* — Remotely-Managed-Device
  - *C* — CVTA
  - *M* — Two-port Mac Relay
- **Platform** — Indicates product name and model number of the neighboring device.

- **Port ID** — Indicates the neighboring device's port from which the CDP packet was sent.

**STEP 2** Select **Enable** in the *CDP Status* field to enable the Cisco Discovery Protocol on the device.

**STEP 3** Define a VLAN ID to be advertised by the device in the *Voice VLAN* field.

**STEP 4** Click **Apply**. CDP is enabled, and the device is updated.

To view additional neighboring device CDP information:

**STEP 1** Click **Monitor & Device Properties > CDP**. The *CDP Page* opens.

**STEP 2** Click **Details**. The *CDP Neighbors Details Page* opens:

#### CDP Neighbors Details Page

Neighbors Details	
Device ID	irena
Advertisement Version	2
Native VLAN	1
Duplex	Full
IP Address	10.5.234.214
Platform	ESW-520-48
Capabilities	S I D
Interface	g9
Port ID (outgoing port)	g1
Time To Live	125 sec
Version	2.1.6

In addition to the fields in the *CDP Page*, the *CDP Neighbors Details Page* contains the following additional fields:

- **Device ID** — Indicates the name of the neighbor device and either the MAC address or the serial number of the device.

- **Advertisement Version** — Indicates the CDP version advertised by the neighboring device.
- **Native VLAN** — Defines the ID number of the VLAN on the neighbor device.
- **Duplex** — Displays the duplex state of connection between the current device and the neighbor device. The possible field values are:
  - *Full* — Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
  - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **IP Address** — Indicates the IP address advertised by the neighboring device.
- **Platform** — Indicates the product name and number of the neighboring device.
- **Capabilities** — Indicates the device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
- **Interface** — Indicates the protocol and port number of the port on the current device.
- **Port ID (outgoing port)** — Indicates the neighboring device's port from which the CDP packet was sent.
- **Time to Live** — Indicates the amount of time in seconds before the neighboring device CDP information is aged out. The field default is 180 seconds.
- **Version** — Indicates the software version of the neighboring device.

## Defining the Bonjour Discovery Protocol

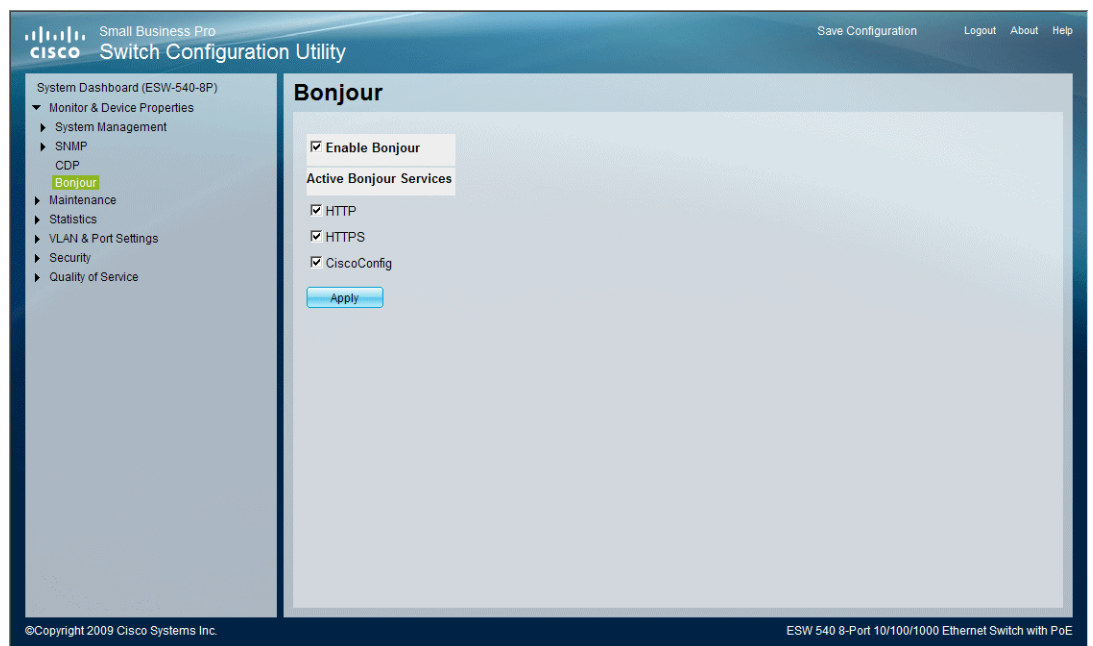
Bonjour is a service discovery protocol that enables automatic discovery of computers, devices, and services on IP networks. Bonjour's multicast Domain Name System (mDNS) service allows the device to publish device services by sending and receiving UDP packets only to the following multicast address 224.0.0.251 and to port number 5353.

The Bonjour screen contains information for enabling/disabling Bonjour on the device, specifying a Service Type and the related port used for publishing devices over the network. A Service Type is the type of service registration performed as part of the device system start up. It is intended to assure the uniqueness of the published service and proclaims the related information. The Service Types that are provided for Bonjour are HTTP, HTTPS, and Cisco Config, a Cisco specific Service Type.

To enable Bonjour on the device:

**STEP 1** Click **Monitor & Device Properties > Bonjour**. The *Bonjour Page* opens:

### Bonjour Page



The Bonjour page contains the following fields:

- **Enable Bonjour** — Specifies whether the switch can publish device services via Bonjour using the mDNS service. The possible field values are:
  - *Checked* — Enables Bonjour on the device. Bonjour is enabled by default.
  - *Unchecked* — Disables Bonjour on the device.
- **Active Bonjour Services** — Specifies the Bonjour services supported by the device. By default all three services are published.

- *HTTP*— Specifies the Service Type selected is HTTP. This service is enabled by default, and can be user-disabled but not deleted. The service uses the default port 80. The port can be changed using the menu CLI.
- *HTTPS*— Specifies the Service Type selected is secured HTTP. This service is enabled by default, and can be user-disabled, but not deleted. The service uses the default port 443. The port can be changed using the menu CLI.
- *CiscoConfig*— Specifies the Service Type selected is CiscoConfig, the Cisco Configuration Service. This service uses the default HTTP port 80. *CiscoConfig* is enabled by default.

**STEP 2** Check **Enable** in the *Enable Bonjour* field to enable Bonjour on the device.

**STEP 3** Check **HTTP** and/or **HTTPS**, and/or **CiscoConfig** in the Active Bonjour Services field.

**STEP 4** Click **Apply**. Bonjour is enabled, and the device is updated.

## TCAM Utilization

The *TCAM Utilization Page* display the availability of Ternary Content Addressable Memory (TCAM) resources. TCAM is used for high-speed searching and performs security, QoS, and other types of applications. In contrast with binary CAM, TCAM allows a third matching state of X or Don't Care bits in data searches. The first two bit types are 0 and 1, adding more flexibility to searches. However, the need to encode three possible states instead of two also adds greater resource costs.

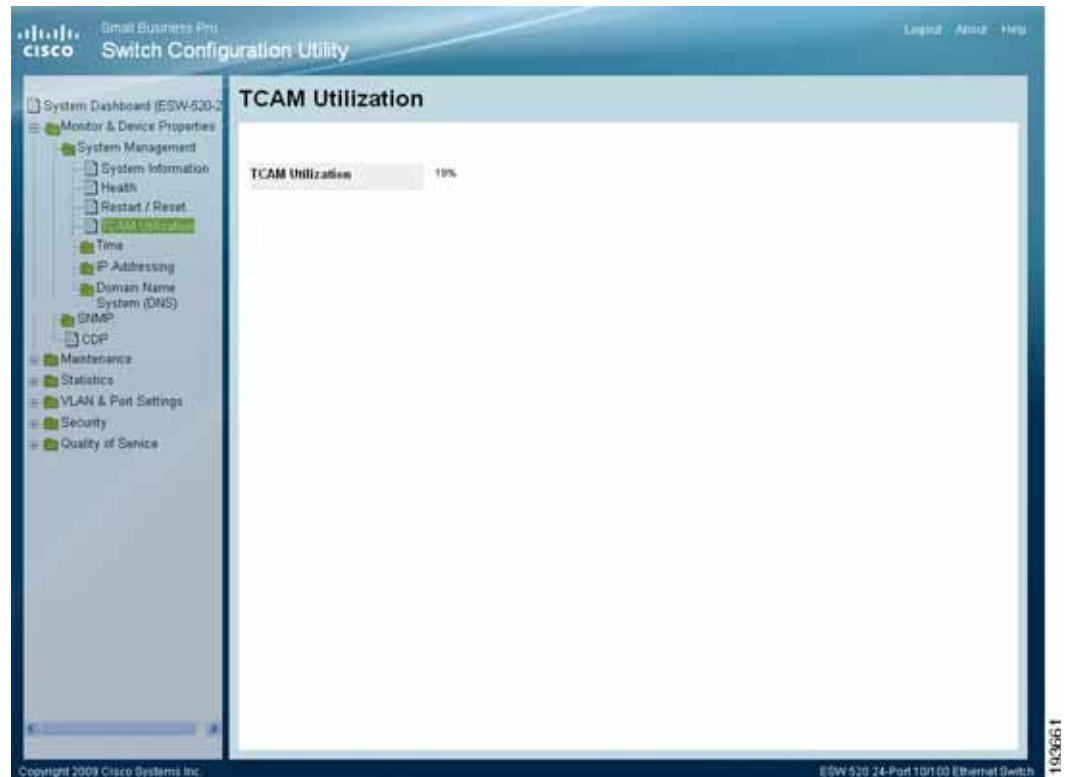
The maximum number of rules that may be allocated by all applications on the device is 1024. Some applications allocate rules upon their initiation. Additionally, applications that initialize during system boot use some of their rules during the startup process.

### TCAM Allocation

To view TCAM Resources:

- STEP 1** Click **Monitor & Device Properties > System Management > TCAM Utilization**. The *TCAM Utilization Page* opens:

#### TCAM Utilization Page



The *TCAM Utilization Page* contains the following field:

- **TCAM Utilization** – Indicates the percentage of the available TCAM resources which are used. For example, if more ACLs and policy maps are defined, the system uses more TCAM resources.

---

# Managing Smart Ports

The Smart Ports wizards provide network managers with quick and simple solution to configuring the devices by understanding and automatically configuring the port settings for various network devices, including:

- **Desktop** — Allows network administrators to define settings for personal desktop users.
- **IP Phone and Desktop** —Allows network administrators to define settings between the switch and the IP Phone. This helps ensure proper network management for voice traffic. The Smart Port IP Phone and Desktop wizard allows network mangers to connect a phone and a PC.
- **Access Point** — Allows network administrators to manage the connection between the device and wireless access points.
- **Switch** — Allows network administrators to manage network settings between switches.
- **Router** — Allows network administrators to manage network settings between routers.
- **Guest** — Allows network administrators to define a port that is connected to a guest.
- **Server** — Allows network administrators to define a port that is connected to a server.
- **Printer** — Allows network administrators to define a port that is connected to a printer.
- **VS Camera** — Allows network administrators to define a port that is connected to a VS camera.
- **Other** — Allows network administrators to remove any previous Smart ports configurations from a port.





**NOTE** By default, the user ports are configured as IP Phone + Desktop for PoE switches and Desktop for non-PoE switches. For devices other than IP Phone and Desktop, users need to configure the smartport role per device (e.g., switch, access point etc.). A port will be deactivated or has degraded service by connecting a switch or an access point to IP phone + desktop smartport respectively because of mismatched port role.

For example, if the network administrator knows that ports 1-10 are access points for a WLAN network, the Smart Ports Wizard is applied to the ports, and the ports are configured with the most common settings for WLAN networks.

Note the following when using the Smart Ports wizard:

- During the Boot Process the Smart Port wizard commands are saved in the Running Configuration file. This ensures that if the device is reset, the Smart Port wizard settings are applied to the ports when the device restarts
- Ports are enabled for the Smart Port wizards by default. However, the initial configuration of the Smart Ports wizards can only occur if the Startup Configuration file is empty.
- If the network administrator modifies the port configuration manually, the Smart ports Wizard may not operate correctly.

## Configuring Smart Ports for Desktops

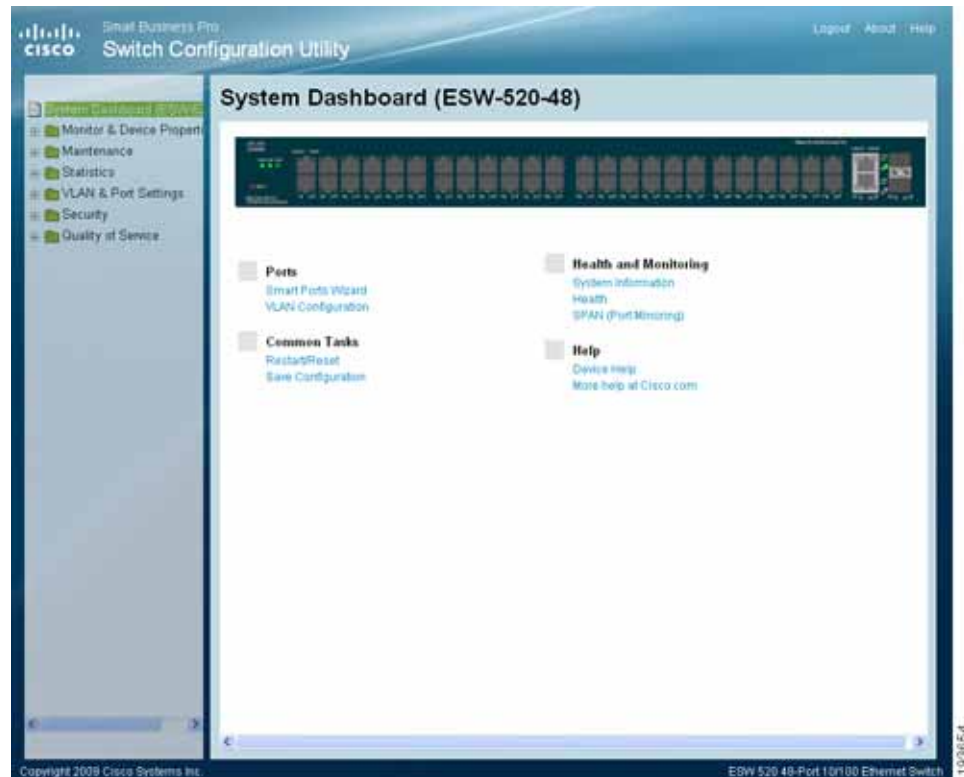
The *Smart Ports for Desktops Page* allows network administrators to define port settings for personal desktop users. To configure ports for desktop users using the Smart Ports Wizard:

## Managing Smart Ports

### Configuring Smart Ports for Desktops

- STEP 1** Open the **Switch Configuration Utility**. The web application automatically opens to the *System Dashboard Page*.

#### System Dashboard Page

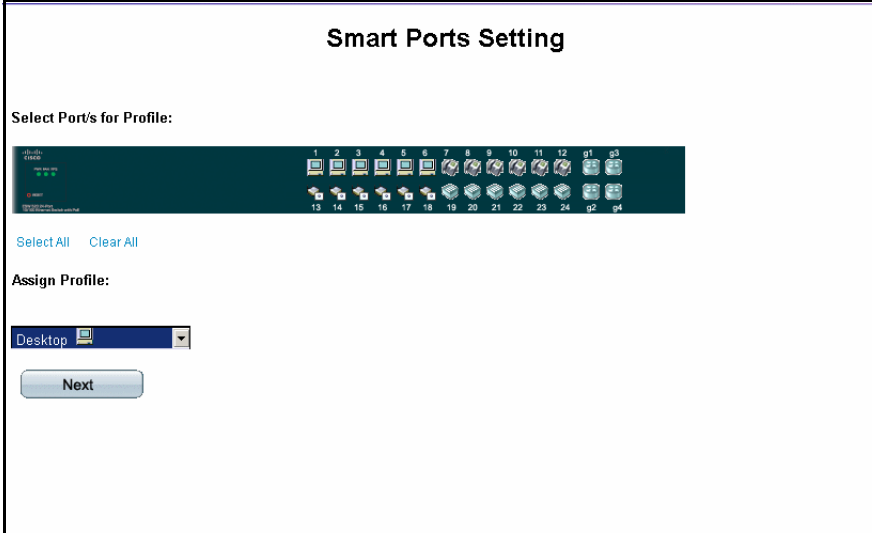


- STEP 2** Click **Smart Ports Wizard** under Ports on the *System Dashboard Page*. The *Smart Ports Setting Page* opens:

## Managing Smart Ports

### Configuring Smart Ports for Desktops

#### Smart Ports Setting Page



The Smart Ports Setting page is a web-based configuration interface. It features a title bar 'Smart Ports Setting'. Below it, the 'Select Port/s for Profile:' section contains a grid of 24 port icons, numbered 1 through 24, arranged in two rows of 12. Below the grid are two links: 'Select All' and 'Clear All'. The 'Assign Profile:' section contains a dropdown menu with 'Desktop' selected. At the bottom is a 'Next' button.

**STEP 3** Select a port or range of ports.

**STEP 4** Select *Desktop* in the *Assign Profile* drop-down list. Click **Next**. The *Smart Ports Desktop Settings Page* opens:

#### Smart Ports Desktops Settings Page



The Smart Ports Desktops Settings page is a web-based configuration interface. It features a title bar 'Desktop'. Below it, there is a table of settings. The table has two columns: 'Ports' and 'g1'. The settings are as follows:

Ports	g1
VLAN Port Mode	Access
VLAN ID	1
Port Security Mode	Dynamic Lock
Max MAC Addresses	1
Port Security Action	Discard
Violation Trap Every	60 Sec
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	general-map
Macro Description	Desktop

At the bottom of the page are two buttons: 'Back' and 'Apply'.

The *Smart Ports Desktops Settings Page* contains the following fields:

- **Port** — Indicates the port to which Smart Port wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The possible value is:

- **Access** — Indicates a port belongs to a single untagged VLAN. This is the default setting for ports that are connected to desktops.
- **VLAN ID** — Indicates the VLAN to which the port belongs.
- **Port Security Mode** — Defines the locked port type. The possible field value is:
  - *Dynamic Lock* — Locks the port with current learned addresses. The dynamic addresses associated with the port are not aged out or relearned on the port as long as the port is locked.
- **Max MAC Addresses** — Indicates the maximum number of MAC addresses that can be learned on the port. The field default is 1.
- **Port Security Actions** — Indicates the action applied to packets arriving on a locked port. The possible field value is:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
- **Violation Trap Every** — Indicates that traps are sent every 60 seconds:
- **Broadcast Storm Control** — Indicates if the percentage of Broadcast Storm Control enabled on the port. The default value is 10% of the port speed.
- **Spanning Tree Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. Port Fast is enabled by default.
- **Spanning Tree BPDU Guard** — Indicates if BPDU Guard is enabled on the interface. BPDU Guard protects the network from invalid configurations. It is usually used either when fast link ports (ports connected to clients) are enabled or when STP is disabled. If a BPDU message is received, the port shuts down and the device generates an appropriate SNMP trap. Spanning Tree BPDU Guard is enabled by default.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The name of the default QoS policy is general-map.
- **Macro Description** — Indicates the type of device connected to the port. For desktops, this field is always Desktop.

**STEP 5** Select a VLAN in the *VLAN ID* drop-down list.

## Managing Smart Ports

### Configuring Smart Ports for IP Phones and Desktops

- STEP 6** Click **Apply**. The Desktop port settings are saved, and the device is updated.

## Configuring Smart Ports for IP Phones and Desktops

The *Smart Ports for IP Phones and Desktops Page* allows network administrators to define settings between the switch and the IP Phone. This helps ensure proper network management for voice traffic. The Smart Port IP Phone and Desktop wizard allows network managers to connect a phone and a PC.

- STEP 1** Open the **Switch Configuration Utility**. The web application automatically opens to the *System Dashboard Page*.
- STEP 2** Click **Smart Ports Wizard** under Ports on the *System Dashboard Page*. The *Smart Ports Setting Page* opens:

### Smart Ports Setting Page

**Smart Ports Setting**

Select Port/s for Profile:

Select All Clear All

Assign Profile:

IP Phone + Desktop

Next

- STEP 3** Select a port or range of ports.
- STEP 4** Select *IP Phone + Desktop* in the *Assign Profile* drop-down list. Click **Next**. The *Smart Ports IP Phones and Desktop Settings Page* opens:

## Managing Smart Ports

### Configuring Smart Ports for IP Phones and Desktops

#### Smart Ports IP Phones and Desktop Settings Page

IP Phone + Desktop	
Ports	g1
VLAN Port Mode	Trunk
Data VLAN	1
Voice VLAN	100
Port Security Mode	Dynamic Lock
Max MAC Addresses	1
Port Security Action	Discard
Violation Trap Every	60 Sec
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	voice-map
Macro Description	IP Phone + Desktop
<div>Back Apply</div>	

The *Smart Ports IP Phones and Desktop Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart Port wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The possible value is:
  - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged. This is the default setting for ports that are connected to desktops and IP phones.
- **Data VLAN** — Defines a specific VLAN as the Data VLAN. Data VLANs only carry data packets and receive a lower priority than voice traffic.
- **Voice VLAN** — Indicates which VLAN is the Voice VLAN. Voice VLANs allows network administrators enhance VoIP service by configuring access ports to carry IP voice traffic from IP phones on specific VLANs.
- **Port Security Mode** — Defines the locked port type. The possible field value is:
  - *Dynamic Lock* — Locks the port with current learned addresses. The dynamic addresses associated with the port are not aged out or relearned on the port as long as the port is locked.

## Managing Smart Ports

### Configuring Smart Ports for IP Phones and Desktops

- **Max MAC Addresses** — Indicates the maximum number of MAC addresses that can be learned on the port. A maximum of 3 MAC addresses can be learned on the port.
- **Port Security Action** — Indicates the action applied to packets arriving on a locked port. The possible field value is:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
- **Violation Trap Every** — Indicates that traps are sent every 60 seconds:
- **Broadcast Storm Control** — Indicates if the percentage of Broadcast Storm Control enabled on the port. The default value is 10% of the port speed.
- **Spanning Tree Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. Fast Port is enabled by default.
- **Spanning Tree BPDU Guard** — Indicates if BPDU Guard is enabled on the interface. BPDU Guard protects the network from invalid configurations. It is usually used either when fast link ports (ports connected to clients) are enabled or when STP is disabled. If a BPDU message is received, the port shuts down and the device generates an appropriate SNMP trap. BPDU guard is enabled by default.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The Default policy is voice-map.
- **Macro Description** — Indicates the type of device connected to the port. For IP Phones + Desktops, this field is always *IP Phones + Desktops*.

**STEP 5** Select a VLAN in the *Data VLAN* drop-down list.

**STEP 6** Click **Apply**. The IP Phone + Desktop port settings are saved, and the device is updated.

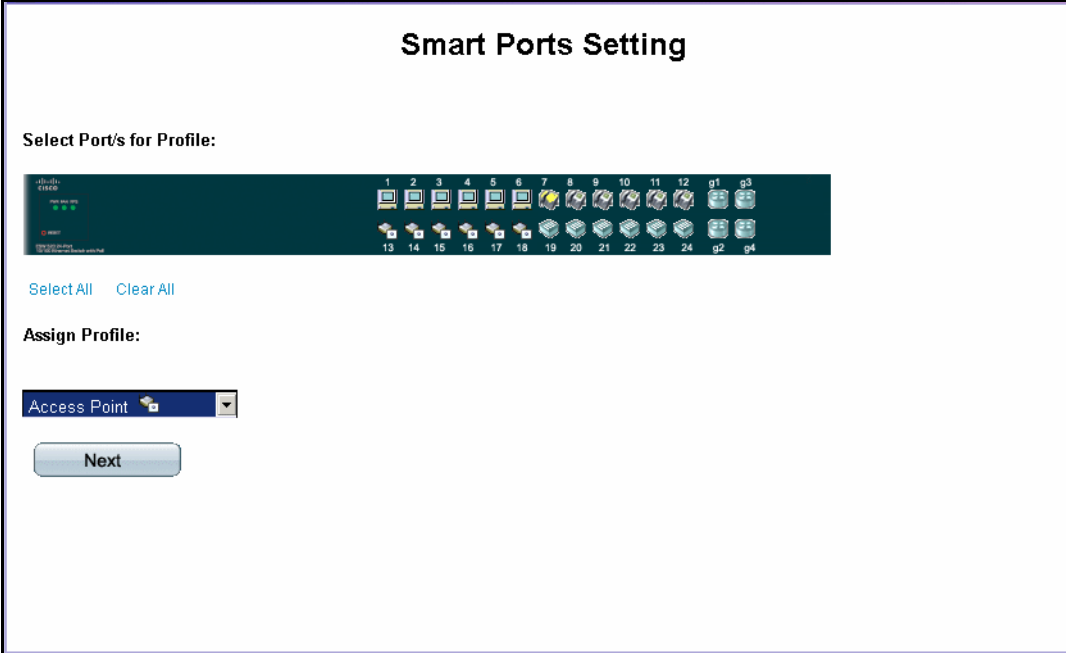
**STEP 7** Click **OK**. The Smart ports Setting page opens.

## Configuring Smart Ports for Access Points

The *Smart Ports for Access Points Page* allows network administrators to manage the connection between the switch and wireless access points. To configure smart ports for access points:

- STEP 1** Open the **Switch Configuration Utility**. The web application automatically opens to the *System Dashboard Page*.
- STEP 2** Click **Smart Ports Wizard** under Ports on the *System Dashboard Page*. The *Smart Ports Setting Page* opens:

### Smart Ports Setting Page



**Smart Ports Setting**

Select Port/s for Profile:

Select All Clear All

Assign Profile:

Access Point

Next

- STEP 3** Select a port or range of ports.
- STEP 4** Select *Access Points* in the *Assign Profile* drop-down list.
- STEP 5** Click **Next**. The Smart Ports Access Point Settings Page opens:.



## Managing Smart Ports

### Configuring Smart Ports for Access Points

#### Smart Ports for Access Points Settings Page

The *Smart Ports for Access Points Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart Port wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The possible value is:
  - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged. This is the default setting for ports that are connected to access points.
- **Trunk Native VLAN ID** — Defines the VLAN receiving untagged packets at ingress.
- **Excluded VLANs** — Defines VLANs that are excluded from receiving untagged packets at egress.
- **Allowed VLANs** — Defines VLANs that are allowed to receive untagged packets at egress.
- **Broadcast Storm Control** — Indicates if the percentage of Broadcast Storm Control enabled on the port. The default value is 10% of the port speed.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The name of the default QoS policy is *general-map*.
- **Macro Description** — Indicates the type of device connected to the port. For access points, this field is always *Access Point*.

**STEP 6** Select a VLAN in the *Trunk Native VLAN ID* drop-down list.

## Managing Smart Ports

### Configuring Smart Ports for Switches

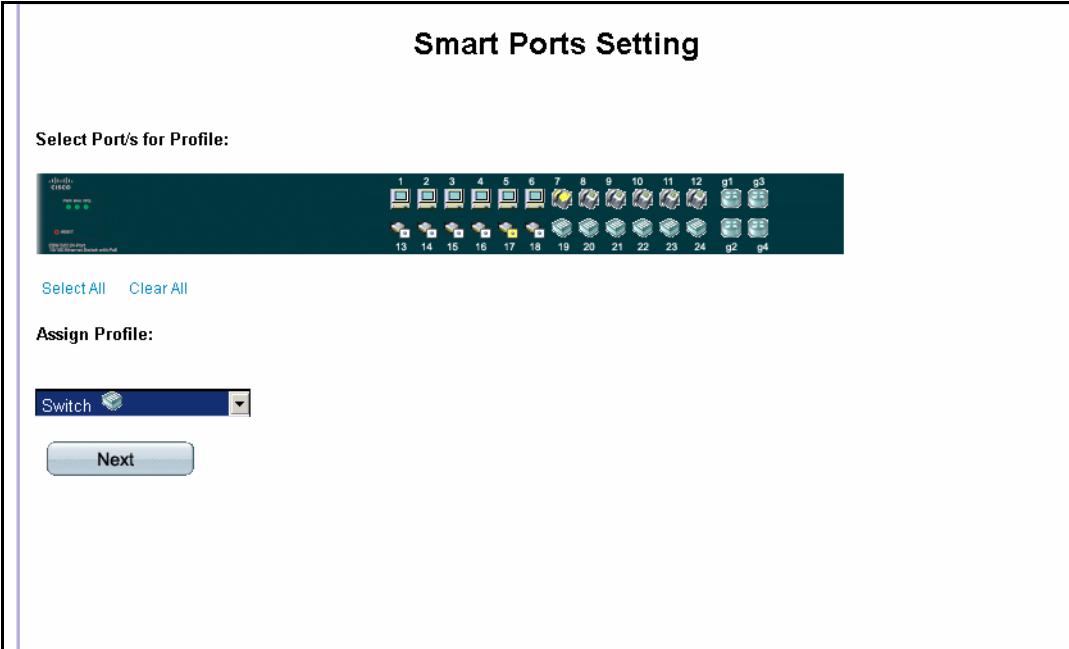
- STEP 7** Select which trunks are permitted in the VLAN using the **Allow** and **Exclude** buttons.
- STEP 8** Click **Apply**. The Access Point port settings are saved, and the device is updated.
- STEP 9** Click **OK**. The Smart ports Setting page opens.

## Configuring Smart Ports for Switches

The *Smart Ports Switch Settings Page* allows network administrators to manage network settings between switches. To configure smart ports for switches:

- STEP 1** Open the **Switch Configuration Utility**. The web application automatically opens to the *System Dashboard Page*.
- STEP 2** Click **Smart Ports Wizard** under Ports on the *System Dashboard Page*. The *Smart Ports Setting Page* opens:

### Smart Ports Setting Page



**Smart Ports Setting**

Select Port/s for Profile:

Select All Clear All

Assign Profile:

Switch

Next

- STEP 3** Select a port or range of ports.

## Managing Smart Ports

### Configuring Smart Ports for Switches

**STEP 4** Select *Switch* in the *Assign Profile* drop-down list. Click **Next**. The *Smart Ports Switch Setting Page* opens:

#### Smart Ports Switch Settings Page

The *Smart Ports Switch Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart Port wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The possible field value is:
  - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged. This is the default setting for ports that are connected to switches.
- **Trunk Native VLAN ID** — Defines the VLAN receiving untagged packets at ingress.
- **Trunk Allowed VLANs** — Defines VLANs that are allowed to receive untagged packets at egress.
- **RSTP Link Type** — Displays the Rapid Spanning Tree Link type. The default value for switches is point-to-point.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The name of the default QoS policy is switch-map.

## Managing Smart Ports

### Configuring Smart Ports for Routers

---

- **Macro Description** — Indicates the type of device connected to the port. For switches, this field is always *Switch*.

**STEP 5** Select a VLAN in the *Trunk Native VLAN ID* drop-down list.

**STEP 6** Select which trunks are permitted in the VLAN using the **Add** and **Delete** buttons.

**STEP 7** Click **Apply**. The switching port settings are saved, and the device is updated.

**STEP 8** Click **OK**. The Smart ports Setting page opens.

---

## Configuring Smart Ports for Routers

The *Smart Port Router Page* allows network administrators to manage network settings between routers. To configure smart ports for routers:

---

**STEP 1** Open the **Switch Configuration Utility**. The web application automatically opens to the *System Dashboard Page*.

**STEP 2** Click **Smart Ports Wizard** under Ports on the *System Dashboard Page*. The *Smart Ports Setting Page* opens:


## Managing Smart Ports

### Configuring Smart Ports for Routers

#### Smart Ports Setting Page

### Smart Ports Setting

Select Port/s for Profile:



1 2 3 4 5 6 7 8 9 10 11 12 g1 g3  
13 14 15 16 17 18 19 20 21 22 23 24 g2 g4

Select All Clear All

Assign Profile:

Router

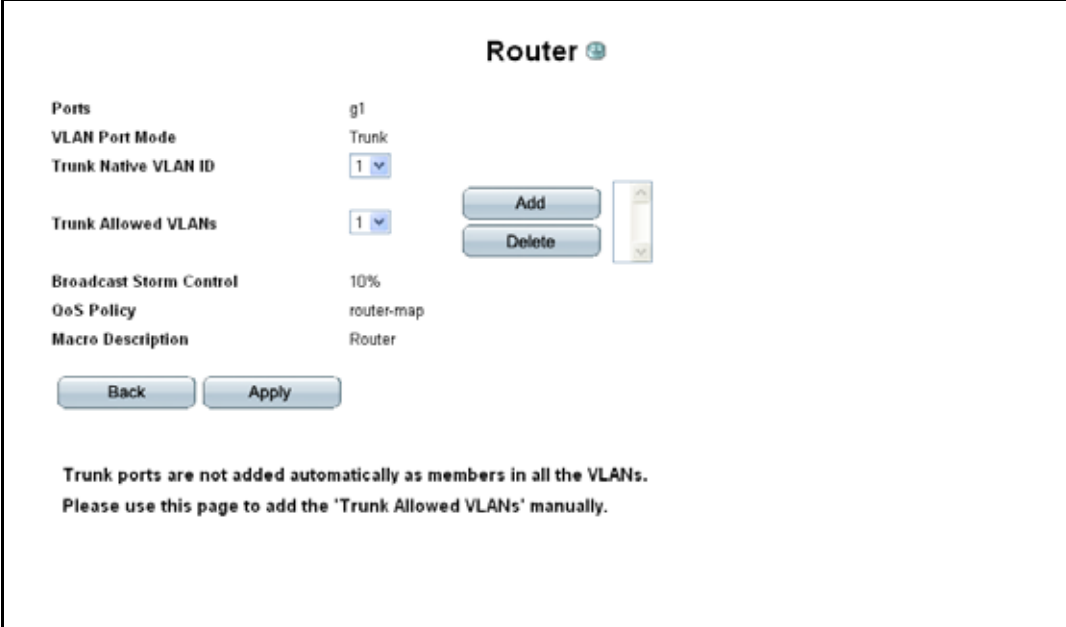
Next

**STEP 3** Select a port or range of ports.

**STEP 4** Select *Router* in the *Assign Profile* drop-down list.

**STEP 5** Click **Next**. The *Smart Port Router Settings Page* opens:

#### Smart Port Router Settings Page



**Router**

Ports	g1
VLAN Port Mode	Trunk
Trunk Native VLAN ID	1
Trunk Allowed VLANs	1
Broadcast Storm Control	10%
QoS Policy	router-map
Macro Description	Router

Back Apply

Trunk ports are not added automatically as members in all the VLANs.  
Please use this page to add the 'Trunk Allowed VLANs' manually.

The *Edit Smart Port Router Page* contains the following fields:

- **Ports** — Indicates the port to which Smart Port wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The possible value is:
  - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged. This is the default setting for ports that are connected to routers.
- **Trunk Native VLAN ID** — Defines the VLAN receiving untagged packets at ingress.
- **Trunk Allowed VLANs** — Defines VLANs that are allowed to receive untagged packets at egress.
- **Broadcast Storm Control** — Indicates if the percentage of Broadcast Storm Control enabled on the port. The default value is 10% of the port speed.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The name of the default QoS policy is router-map.
- **Macro Description** — Indicates the type of device connected to the port. For routers, this field is always *Router*.

**STEP 6** Select a VLAN in the *Trunk Native VLAN ID* drop-down list.

## Managing Smart Ports

### Configuring Smart ports for Guests

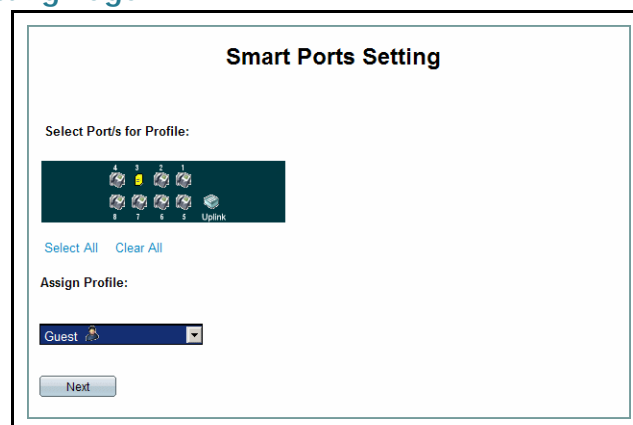
- STEP 7** Select with trunks are permitted in the VLAN using the **Add** and **Delete** buttons.
- STEP 8** Click **Apply**. The routing port settings are saved, and the device is updated.
- STEP 9** Click **OK**. The Smart ports Setting page opens.

## Configuring Smart ports for Guests

The *Smart Ports Setting Page* allows network administrators to manage network settings between the switch and a guest in the company. It is recommended that this connection be restricted to specific applications. To configure Smart ports for a guest:

- STEP 1** Open the **Small Business Pro** web application. The web application automatically opens to the Ports are enabled for the Smart Port wizards by default. However, the initial configuration of the Smart Ports wizards can only occur if the Startup Configuration file is empty..
- STEP 2** Click *Smart ports Wizard* under Ports on the Ports are enabled for the Smart Port wizards by default.
- STEP 3** Select a port or range of ports.
- STEP 4** Select *Guest* in the *Assign Profile* dropdown box.

### Smart ports Setting Page



- STEP 5** Click **Next**. The *Smartports Guest Settings Page* opens:

#### Smartports Guest Settings Page

Guest	
Ports	g3
VLAN Port Mode	Access
Trunk Native VLAN ID	1
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	guest-map
Macro Description	Guest

Back Apply

The *Smartports Guest Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart ports Wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The value is:
  - *Access* — Indicates the value is Access.
- **Trunk Native VLAN ID** — Defines the VLAN receiving untagged packets at ingress. The default value is VLAN 1. The user can change it to any other created VLAN through a drop down list.
- **Broadcast Storm Control** — Indicates the percentage of Broadcast Storm Control enabled on the port. The value is 10% of the port speed.
- **Spanning Tree Port Fast** — Indicates Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.
- **Spanning Tree BPDU Guard** — Indicates if BPDU Guard is enabled on the interface.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The name of the default QoS policy is router-map.
- **Macro Description** — Indicates the type of device connected to the port. For guests, this field is always *Guest*.

**STEP 6** Select a VLAN in the *VLAN ID* dropdown box.

**STEP 7** Click **Apply**. The guest port settings are saved, and the device is updated.

**STEP 8** Click OK. The *Smart ports Setting* page opens.



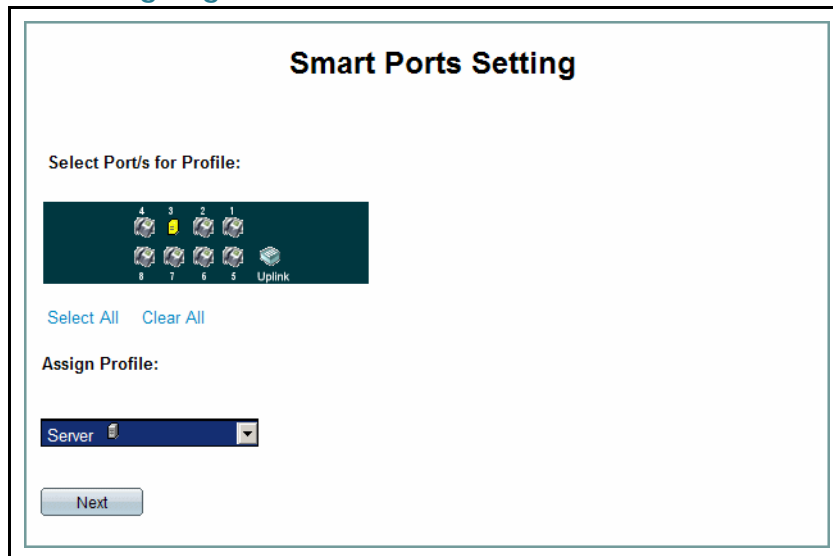
## Configuring Smart ports for Servers

The *Smart ports Setting Page* allows network administrators to define settings between the device and a server.

To configure ports using the Server:

- STEP 1** Open the **Small Business Pro** web application. The web application automatically opens to the Ports are enabled for the Smart Port wizards by default. However, the initial configuration of the Smart Ports wizards can only occur if the Startup Configuration file is empty..
- STEP 2** Click Smart ports Wizard under Ports on the *Ports are enabled for the Smart Port wizards by default*.
- STEP 3** Select a port or range of ports.
- STEP 4** Select *Server* in the *Assign Role dropdown* box.

### Smart ports Setting Page



**Smart Ports Setting**

Select Port/s for Profile:

4 3 2 1  
8 7 6 5 Uplink

Select All Clear All

Assign Profile:

Server

Next

- STEP 5** Click **Next**. The *Smart ports Server Settings Page* opens:

#### Smart ports Server Settings Page

Server 0	
Ports	e8
VLAN Port Mode	Access
Trunk Native VLAN ID	1
Port Security Mode	Dynamic Lock
Max MAC Addresses	3
Port Security Action	Discard
Violation Trap Every	60 Sec
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	general-map
Macro Description	Server

Back Apply

The *Smart ports Server Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart ports Wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The value is:
  - *Access* — Indicates the value is Access.
- **Trunk Native VLAN ID** — Indicates the VLAN to which the port belongs. The default is VLAN 1 – the user can change this VLAN by selecting one of the created VLANs via the drop down list.
- **Port Security Mode** — Defines the locked port type. The field value is: *Dynamic Lock*.
- **Max MAC Addresses** — Indicates the maximum number of MAC addresses that can be learned on the port. A maximum of three MAC addresses can be learned on the port.
- **Port Security Action** — Indicates the action applied to packets arriving on a locked port. The value is:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
- **Violation Trap Every** — Indicates that traps are sent every 60 seconds.
- **Broadcast Storm Control** — Indicates the percentage of Broadcast Storm Control enabled on the port. The value is 10% of the port speed.
- **Spanning Tree Port Fast** — Indicates Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the

Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.

- **Spanning Tree BPDU Guard** — Indicates if BPDU Guard is enabled on the interface.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The Default policy is voice-map.
- **Macro Description**— Indicates the type of device connected to the port. For servers, this field is always *Server*.

**STEP 6** Select a VLAN in the *VLAN ID* dropdown box.

**STEP 7** Click **Apply**. The Server port settings are saved, and the device is updated.

**STEP 8** Click OK. The *Smart ports Setting* page opens.

## Configuring Smart ports for Printers

The *Smart ports Setting Page* allows network administrators to define settings between the device and a printer.

To configure ports using the printer:

**STEP 1** Open the **Small Business Pro** web application. The web application automatically opens to the *Ports are enabled for the Smart Port wizards by default. However, the initial configuration of the Smart Ports wizards can only occur if the Startup Configuration file is empty.*

**STEP 2** Click Smart ports Wizard under Ports on the *Ports are enabled for the Smart Port wizards by default.*

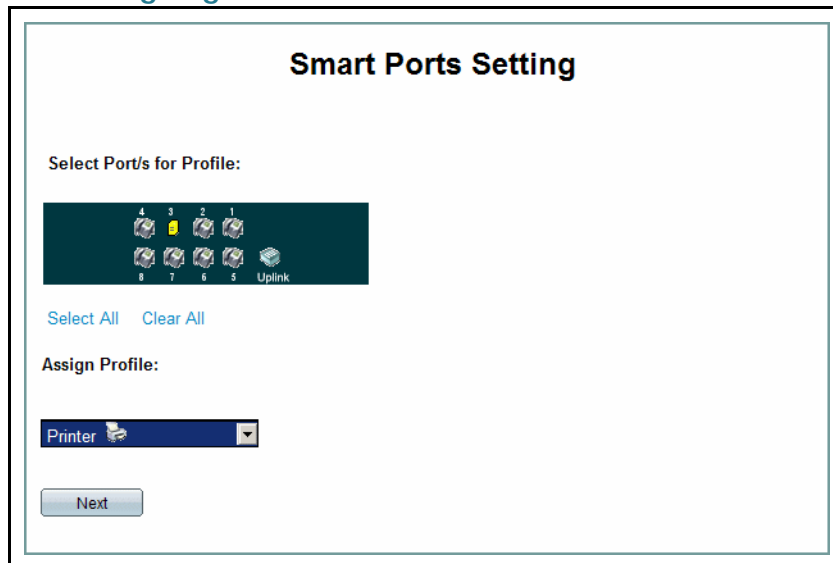
**STEP 3** Select a port or range of ports.

**STEP 4** Select *Printer* in the *Assign Role* dropdown box.

## Managing Smart Ports

### Configuring Smart ports for Printers

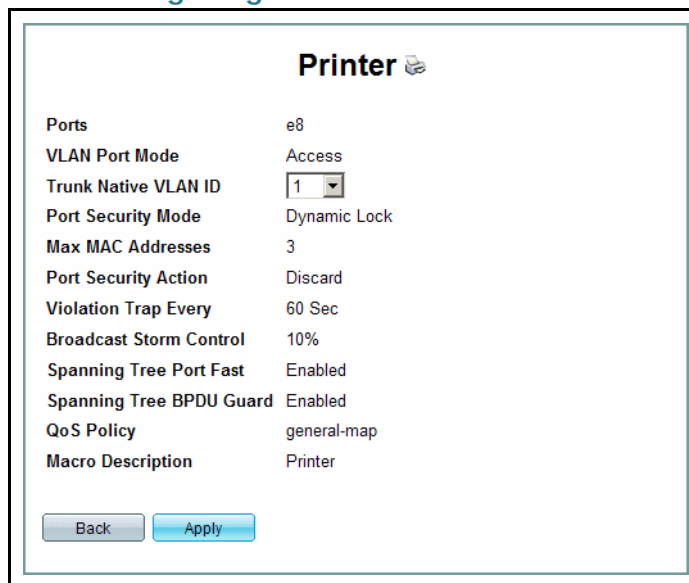
#### Smart ports Setting Page



The screenshot shows the 'Smart Ports Setting' page. At the top, it says 'Smart Ports Setting'. Below that, there is a section 'Select Port/s for Profile:' with a grid of port icons. Port 3 is highlighted in yellow. Below the grid are links for 'Select All' and 'Clear All'. Underneath is the 'Assign Profile:' section with a dropdown menu showing 'Printer'. At the bottom is a 'Next' button.

**STEP 5** Click **Next**. The *Smartports Printer Settings Page* opens:

#### Smartports Printer Settings Page



The screenshot shows the 'Printer' settings page. The title is 'Printer' with a printer icon. Below the title is a table of settings:

Ports	e8
VLAN Port Mode	Access
Trunk Native VLAN ID	1
Port Security Mode	Dynamic Lock
Max MAC Addresses	3
Port Security Action	Discard
Violation Trap Every	60 Sec
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	general-map
Macro Description	Printer

At the bottom are 'Back' and 'Apply' buttons.

The *Smartports Printer Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart ports Wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The value is:
  - *Access* — Indicates the value is Access.

- **Trunk Native VLAN ID** — Indicates the VLAN to which the port belongs. The default is VLAN 1 – the user can change this VLAN by selecting one of the created VLANs via the drop down list.
- **Port Security Mode** — Defines the locked port type. The field value is: *Dynamic Lock*.
- **Max MAC Addresses** — Indicates the maximum number of MAC addresses that can be learned on the port. A maximum of three MAC addresses can be learned on the port.
- **Port Security Action** — Indicates the action applied to packets arriving on a locked port. The value is:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
- **Violation Trap Every** — Indicates that traps are sent every 60 seconds.
- **Broadcast Storm Control** — Indicates the percentage of Broadcast Storm Control enabled on the port. The value is 10% of the port speed.
- **Spanning Tree Port Fast** — Indicates Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.
- **Spanning Tree BPDU Guard** — Indicates if BPDU Guard is enabled on the interface.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The Default policy is voice-map.
- **Macro Description**— Indicates the type of device connected to the port. For printers, this field is always *Printer*.

**STEP 6** Select a VLAN in the *VLAN ID* dropdown box.

**STEP 7** Click **Apply**. The Server port settings are saved, and the device is updated.

**STEP 8** Click OK. The *Smart ports Setting* page opens.

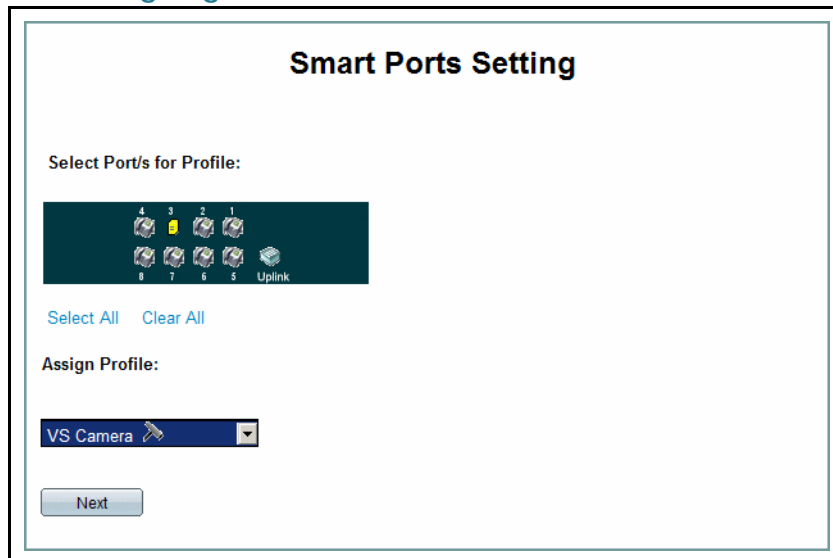
## Configuring Smart ports for VS Camera

The *Smart ports Setting Page* allows network administrators to define settings between the device and a video surveillance camera.

To configure ports using a VS camera:

- STEP 1** Open the **Small Business Pro** web application. The web application automatically opens to the *Ports are enabled for the Smart Port wizards by default. However, the initial configuration of the Smart Ports wizards can only occur if the Startup Configuration file is empty.*
- STEP 2** Click Smart ports Wizard under Ports on the *Ports are enabled for the Smart Port wizards by default.*
- STEP 3** Select a port or range of ports.
- STEP 4** Select *VS Camera* in the *Assign Role* dropdown box.

### Smart ports Setting Page



**Smart Ports Setting**

Select Port/s for Profile:

4 3 2 1  
8 7 6 5 Uplink

Select All Clear All

Assign Profile:

VS Camera

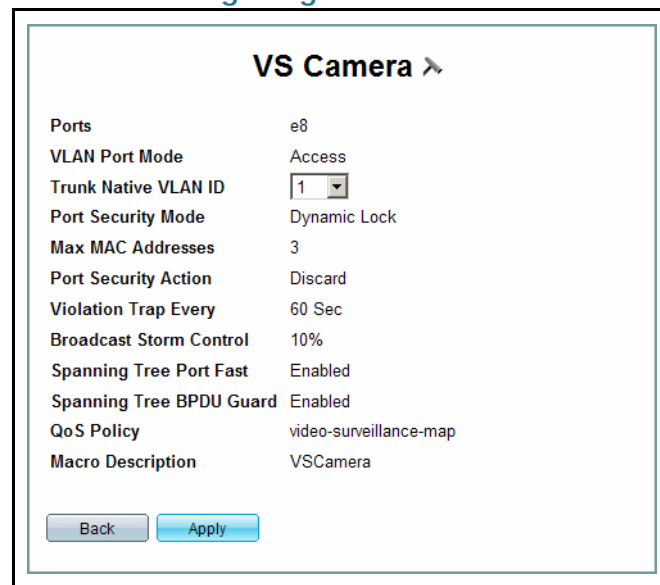
Next

- STEP 5** Click **Next**. The *Smartports VS Camera Settings Page* opens:

## Managing Smart Ports

### Configuring Smart ports for VS Camera

#### Smart ports VS Camera Settings Page



The screenshot shows a configuration window titled "VS Camera" with a mouse cursor icon. It contains a list of settings for a smart port. At the bottom are "Back" and "Apply" buttons.

Setting	Value
Ports	e8
VLAN Port Mode	Access
Trunk Native VLAN ID	1
Port Security Mode	Dynamic Lock
Max MAC Addresses	3
Port Security Action	Discard
Violation Trap Every	60 Sec
Broadcast Storm Control	10%
Spanning Tree Port Fast	Enabled
Spanning Tree BPDU Guard	Enabled
QoS Policy	video-surveillance-map
Macro Description	VSCamera

The *Smart ports Server Settings Page* contains the following fields:

- **Ports** — Indicates the port to which Smart ports Wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The value is:
  - *Access* — Indicates the value is Access.
- **Trunk Native VLAN ID** — Indicates the VLAN to which the port belongs. The default is VLAN 1 – the user can change this VLAN by selecting one of the created VLANs via the drop down list.
- **Port Security Mode** — Defines the locked port type. The field value is: *Dynamic Lock*.
- **Max MAC Addresses** — Indicates the maximum number of MAC addresses that can be learned on the port. A maximum of three MAC addresses can be learned on the port.
- **Port Security Action** — Indicates the action applied to packets arriving on a locked port. The value is:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
- **Violation Trap Every** — Indicates that traps are sent every 60 seconds.
- **Broadcast Storm Control** — Indicates the percentage of Broadcast Storm Control enabled on the port. The value is 10% of the port speed.

- **Spanning Tree Port Fast** — Indicates Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.
- **Spanning Tree BPDU Guard** — Indicates if BPDU Guard is enabled on the interface.
- **QoS Policy** — Indicates that the default QoS policy settings are applied to the port. The Default policy is voice-map.
- **Macro Description**— Indicates the type of device connected to the port. For VS cameras, this field is always *VS Camera*.

**STEP 6** Select a VLAN in the *VLAN ID* dropdown box.

**STEP 7** Click **Apply**. The Server port settings are saved, and the device is updated.

**STEP 8** Click OK. The *Smart ports Setting* page opens.

## Configuring Smart Ports for Other

The *Smart Port Other Page* allows network administrators to remove any previous Smart Ports configuration from a port.

You can also use the smart ports for other setting to analyze network traffic. You can analyze network traffic passing through ports or by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. The following are the steps to set up port mirroring:

**STEP 1** Select the destination port. Configure the port as Other

**STEP 2** Connect the destination port to a computer with Wireshack network protocol analyzer.

**STEP 3** Go to **Maintenance -> Diagnostics -> SPAN (Port Monitoring)**. Configure the destination port and source port together with traffic type.

**STEP 4** Monitor the source ports traffic by Wireshack.



## Managing Smart Ports

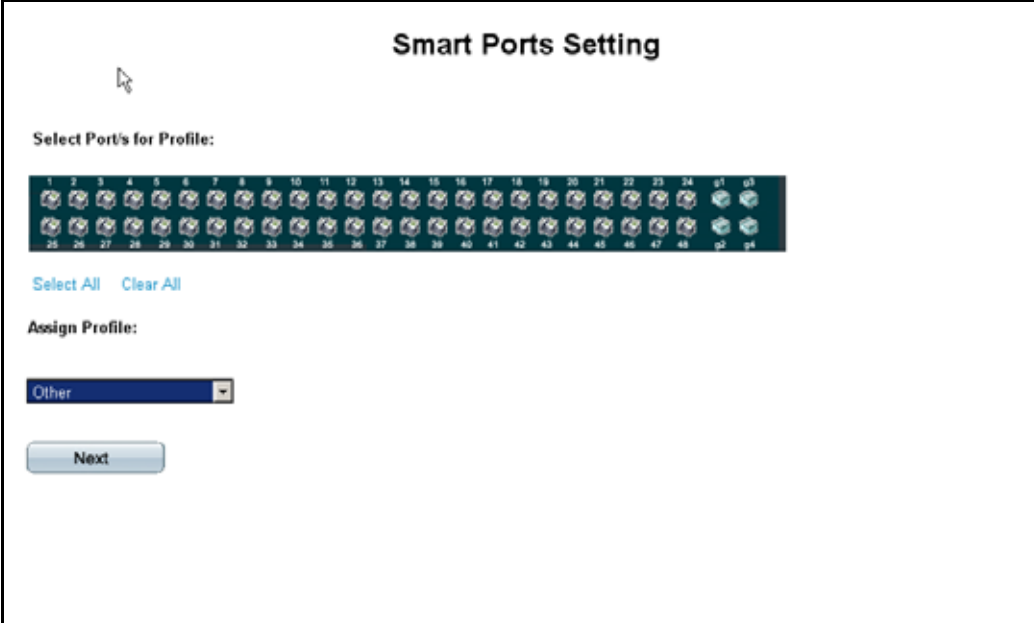
### Configuring Smart Ports for Other

For more information on configuring SPAN (Port Mirroring), see Chapter 19, Managing Device Diagnostics.

To remove any previous Smart Ports configuration from a port, configure smart ports for other:

- STEP 1** Open the **Switch Configuration Utility**. The web application automatically opens to the *System Dashboard Page*.
- STEP 2** Click **Smart Ports Wizard** under Ports on the *System Dashboard Page*. The *Smart Ports Setting Page* opens:

#### Smart Ports Settings Page



- STEP 3** Select a port or range of ports.
- STEP 4** Select Other in the *Assign Profile* drop-down list.
- STEP 5** Click **Next**, the Other page opens.

## Managing Smart Ports

### Configuring Smart Ports for Other

#### Smart Ports Other Page

The screenshot shows a configuration window titled "Other". It contains the following fields and controls:

Ports	g1
VLAN Port Mode	Access
VLAN ID	1
Macro Description	Other

At the bottom of the form are two buttons: "Back" and "Apply".

The *Edit Smart Port Other Page* contains the following fields:

- **Ports** — Indicates the port to which Smart Port wizard settings are applied.
- **VLAN Port Mode** — Indicates the VLAN port mode enabled on the port. The possible value is:
  - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged. This is the default setting for ports that are connected to routers.
- **Trunk Native VLAN ID** — Defines the VLAN receiving untagged packets at ingress. The default value is VLAN 1, the user can change it to any other created VLAN through a drop down list.
- **Macro Description** — Displays Other, which indicates the port has no Wizard configured.

**STEP 6** Select a VLAN in the *VLAN ID* drop-down list.

**STEP 7** Click **Apply**. The port settings are saved, and the device is updated.

# Configuring System Time

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client, and cannot provide time services to other systems.

This section provides information for configuring the system time, and includes the following topics:

- Defining System Time
- Defining SNTP Settings
- Defining SNTP Authentication

## Defining System Time

The *System Time Page* contains fields for defining system time parameters for both the local hardware clock, and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device.

To define system time:

## Configuring System Time

### Defining System Time

- STEP 1** Click **Monitor & Device Properties > System Management > Time > System Time**. The *System Time Page* opens:

#### System Time Page

The screenshot shows the Cisco Switch Configuration Utility interface. On the left is a navigation tree with categories like System Dashboard, Monitor & Device Properties, System Management, Time, and others. The 'Time' category is selected, and the 'System Time' page is displayed. The page has a title bar 'System Time' and a 'Clock Source' section with two radio buttons: 'Use Local Settings' (selected) and 'Use NTP Server'. Below this is the 'Local Settings' section with fields for 'Date' (11 Mar 09), 'Local Time' (10:41:45), and 'Time Zone Offset' (GMT). There are also checkboxes for 'Daylight Saving' and 'Time Set Offset' (0 min). At the bottom, there are 'From' and 'To' fields for recurring time settings, each with a 'Day', 'Week', 'Month', and 'Time' sub-field. An 'Apply' button is at the bottom center. The footer of the page includes 'Copyright 2009 Cisco Systems Inc.' and 'ESW 520 48-Port 10/100 Ethernet Switch'.

The *System Time Page* contains the following fields:

- **Clock Source** — Indicates the source used to set the system clock. The possible field values:
  - *Use Local Settings* — The system time is set on the local device. This is the default value.
  - *Use NTP Server* — Sets the system time via an NTP server.
- **Date** — Indicates the system date. The field format is DD/MMM/YY, for example, 12/Dec/08.
- **Local Time** — Indicates the system time. The field format is HH:MM:SS, for example, 21:15:03.
- **Time Zone Offset** — Indicates the difference between *Greenwich Mean Time* (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1,

while the local time in New York is GMT –5. There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the *Daylight Savings* area, and for a recurring setting, complete the *Recurring* area.

- **Daylight Savings** — Enables the Daylight Savings Time (DST) on the device based on the devices location. The possible field values are:
  - *USA* — The device switches to DST 2 a.m. on the second Sunday of March, and reverts to standard time at 2 a.m. on the first Sunday in November.
  - *European* — The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The *European* option applies to EU members, and other European countries using the EU standard.
  - *Other* — The DST definitions are user-defined based on the device locality. If Other is selected, the *From* and *To* fields must be defined.
- **Time Set Offset (1-1440)** — Indicates the difference in minutes between DST and the local standard time. The default time is 60 minutes.

The following fields are active for non-USA and European countries.

- **From** — Indicates the time that DST ends in countries other than USA or Europe in the Day:Month:Year format in one field and time in another. For example, DST begins on the 25th October 2007 5:00 am, the two fields will be 25/Oct/07 and 5:00. The possible field values are:
  - *Date* — The date at which DST begins. The possible field range is 1-31.
  - *Month* — The month of the year in which DST begins. The possible field range is Jan-Dec.
  - *Year* — The year in which the configured DST begins.
  - *Time* — The time at which DST begins. The field format is Hour:Minute, for example, 05:30.
- **To** — Indicates the time that DST ends in countries other than USA or Europe in the Day:Month:Year format in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields will be 23/Mar/08 and 12:00. The possible field values are:
  - *Date* — The date at which DST ends. The possible field range is 1-31.

- *Month* — The month of the year in which DST ends. The possible field range is Jan-Dec.
  - *Year* — The year in which the configured DST ends.
  - *Time* — The time at which DST starts. The field format is Hour:Minute, for example, 05:30.
- **Recurring** — Select if the DST period in countries other than USA or European is constant from year to year. The possible field values are:
- **From** — Indicates the day and time that DST begins each year. For example, DST begins locally every second Sunday in April at 5:00 am. The possible field values are:
  - *Day* — The day of the week from which DST begins every year. The possible field range is Sunday- Saturday.
  - *Week* — The week within the month from which DST begins every year. The possible field range is First, 2,3,4, Last.
  - *Month* — The month of the year in which DST begins every year. The possible field range is Jan.-Dec.
  - *Time* — The time at which DST begins every year. The field format is Hour:Minute, for example, 02:10.
- **To** — Indicates the day and time that DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The possible field values are:
  - *Day* — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
  - *Week* — The week within the month at which DST ends every year. The possible field range is First, 2,3,4, Last.
  - *Month* — The month of the year in which DST ends every year. The possible field range is Jan.-Dec.
  - *Time* — The time at which DST ends every year. The field format is Hour:Minute, for example, 05:30.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The Time Settings are defined, and the device is updated.

## Defining SNTP Settings

The *SNTP Settings Page* contains information for enabling SNTP servers, as well as adding new SNTP servers. In addition, the *SNTP Settings Page* enables the device to request and accept SNTP traffic from a server. To define SNTP global settings:

- STEP 1** Click **Monitor & Device Properties > System Management > Time > SNTP Settings**. The *SNTP Settings Page* opens:

### SNTP Settings Page



The *SNTP Settings Page* contains the following fields:

- **Enable SNTP Broadcast Reception** — Enables polling the selected SNTP Server for system time information.
- **SNTP Server** — Indicates the SNTP server IP address. Up to eight SNTP servers can be defined.
- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for system time information. By default, the poll interval is 1024 seconds.

- **Encryption Key ID** — Indicates the Key Identification used to communicate between the SNTP server and device. The range is 1 - 4294967295.
- **Preference** — The SNTP server providing SNTP system time information. The possible field values are:
  - *Primary* — The primary server provides SNTP information.
  - *Secondary* — The backup server provides SNTP information.
  - *In progress* — The SNTP server is currently sending or receiving SNTP information.
  - *Unknown* — The progress of the SNTP information currently being sent is unknown. For example, the device is currently trying to locate an interface.
- **Status** — The operating SNTP server status. The possible field values are:
  - *Up* — The SNTP server is currently operating normally.
  - *Down* — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.
  - *Unknown* — Indicates that the device (sntp client) is currently looking for sntp server.
- **Last Response** — Indicates the last time a response was received from the SNTP server.
- **Offset** — Indicates the difference in minutes between DST and the local standard time. The default time is 60 minutes.
- **Delay** — Indicates the amount of time it takes to reach the SNTP server.

**STEP 2** Click the **Add** button. The *Add SNTP Server Page* opens:



#### Add SNTP Server Page

The screenshot shows a web-based configuration page titled "Add SNTP Server". It contains three main fields: "SNTP Server" with a text input box, "IP Address" with a text input box, and "Enable Poll Interval" with a checkbox. Below these is an "Encryption Key ID" field with a dropdown menu. An "Apply" button is located at the bottom right of the form area. The page number "103447" is visible in the bottom right corner.

The *Add SNTP Server Page* contains the following fields:

- **SNTP Server** — The SNTP server's IP address.
- **Enable Poll Interval** — Select whether or not the device polls the selected SNTP server for system time information.
- **Encryption Key ID** — Select if Key Identification is used to communicate between the SNTP server and device. The range is 1 - 4294967295.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNTP Server is added, and the device is updated.

## Defining SNTP Authentication

The *SNTP Authentication Page* provides parameters for performing authentication of the SNTP server.

- STEP 1** Click **Monitor & Device Properties > System Management > Time > SNTP Authentication**. The *SNTP Authentication Page* opens:

#### SNTP Authentication Page

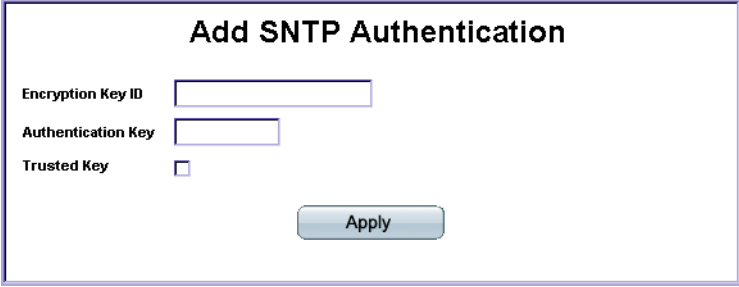


The *SNTP Authentication Page* contains the following fields:

- **Enable SNTP Authentication** — Indicates if authenticating an SNTP session between the device and an SNTP server is enabled on the device. The possible field values are:
  - *Checked* — Authenticates SNTP sessions between the device and SNTP server.
  - *Unchecked* — Disables authenticating SNTP sessions between the device and SNTP server.
- **Encryption Key ID** — Indicates the Key Identification used to authenticate the SNTP server and device. The range is 1 - 4294967295.
- **Authentication Key** — Displays the key used for authentication.
- **Trusted Key** — Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.

- STEP 2** Click the **Add** button. The *Add SNTP Authentication Page* opens:

#### Add SNTP Authentication Page



The screenshot shows a web form titled "Add SNTP Authentication". It contains three input fields: "Encryption Key ID" (a text box), "Authentication Key" (a text box), and "Trusted Key" (a checkbox). Below these fields is a blue "Apply" button.

The *Add SNTP Authentication Page* contains the following fields:

- **Encryption Key ID** — Defines the Key Identification used to authenticate the SNTP server and device. The range is 1 - 4294967295.
- **Authentication Key** — Defines the key used for authentication.
- **Trusted Key** — Indicates if an encryption key is used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNTP Authentication is defined, and the device is updated.

---

# Configuring Device Security

The Security Suite contains the following topics:

- Passwords Management
- Defining Authentication
- Defining Access Methods
- Defining Traffic Control
- Defining 802.1x
- Defining Access Control
- Defining DoS Prevention
- Defining DHCP Snooping
- Defining Dynamic ARP Inspection

## Passwords Management

This section contains information for defining passwords. Passwords are used to authenticate users accessing the device. By default, a single user name is defined, *cisco*, with a password of *cisco*.



---

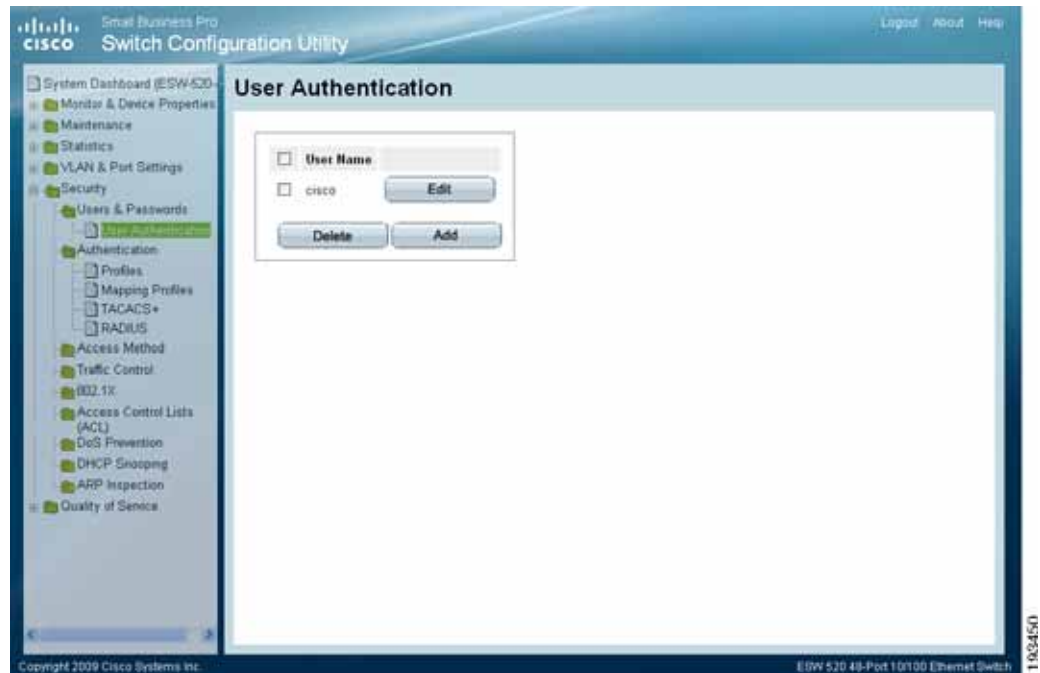
**NOTE** When a new Local User is added, the default user name, *cisco* will be overwritten.

---

To define Passwords:

- STEP 1** Click **Security > Users and Passwords > User Authentication**. The *User Authentication Page* opens:

#### User Authentication Page



The *User Authentication Page* contains the following fields:

- **User Name** — Displays the user name.

- STEP 2** Click the **Add** button. The *Add Local User Page* opens:

#### Add Local User Page

### Add Local User

User Name	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>

Apply

The *Add Local User Page* contains the following fields:

- **User Name** — Specifies the user name.
- **Password** — Specifies the new password. The password is not displayed. As it is entered an \* corresponding to each character is displayed in the field. (Range: 1-159 characters)
- **Confirm Password** — Confirms the new password. The password entered into this field must be exactly the same as the password entered in the **Password** field.

**STEP 3** Define the relevant fields

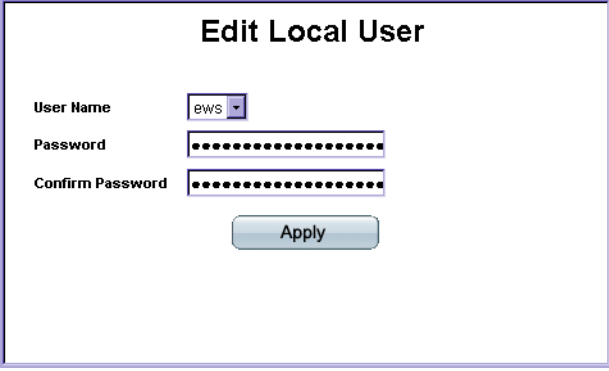
**STEP 4** Click **Apply**. The local user settings are modified, and the device is updated..

## Modifying the Local User Settings

**STEP 1** Click **Security > Users and Passwords > User Authentication**. The *User Authentication Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit Local User Page* opens:

### Edit Local User Page



The screenshot shows a web form titled "Edit Local User". It contains three input fields: "User Name" with a dropdown menu showing "EWS", "Password" with a masked input (dots), and "Confirm Password" with a masked input (dots). Below the fields is an "Apply" button.

The *Edit Local User Page* contains the following fields:

- **User Name** — Specifies the user name.
- **Password** — Specifies the new password. The password is not displayed. As it entered an \* corresponding to each character is displayed in the field. (Range: 1-159 characters)
- **Confirm Password** — Confirms the new password. The password entered into this field must be exactly the same as the password entered in the **Password** field.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The local user settings are modified, and the device is updated.

## Defining Authentication

The Authentication section contains the following pages:

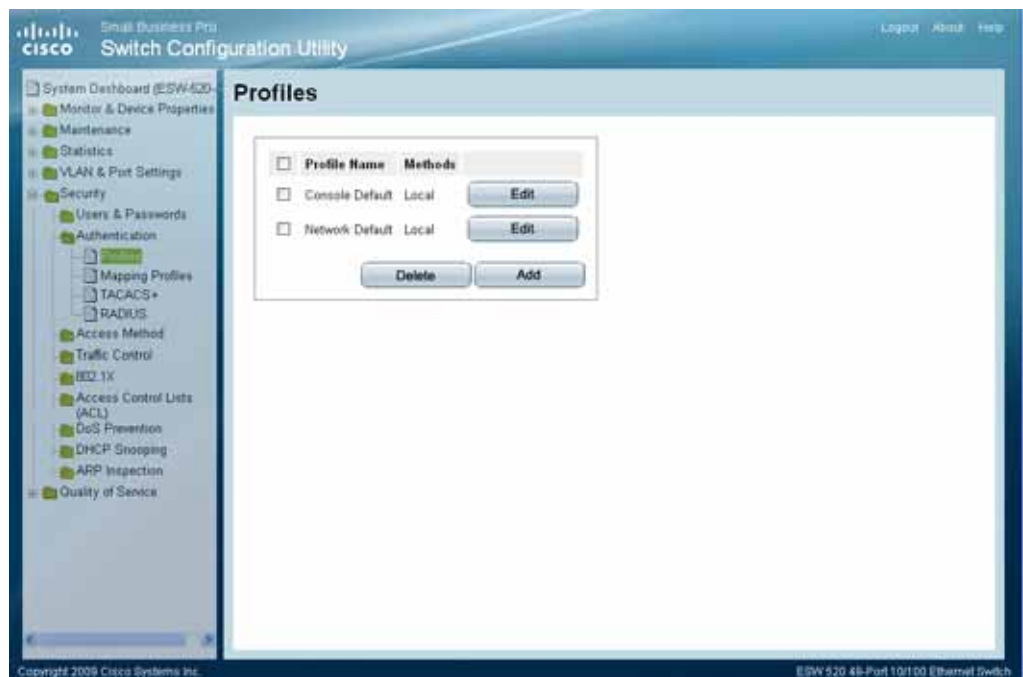
- Defining Profiles
- Mapping Authentication Profiles
- Defining TACACS+
- Defining RADIUS

### Defining Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally.

**STEP 1** Click **Security > Authentication > Profiles**. The *Profiles Page* opens:

#### Profiles Page



The *Profiles Page* contains the following fields:

- **Profile Name** — Displays the Profile name defined for the Login Table.
- **Methods** — Defines the user authentication methods. The order of the authentication methods defines the order in which authentication is attempted. For example, if the authentication method order is RADIUS, Local, the system first attempts to authenticate the user on a RADIUS server. If there is no available RADIUS server, then authentication is attempted on the local data base. Note that if the RADIUS server is available, but authentication fails, then the user is denied access. The possible field values are:
  - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
  - *RADIUS* — Authenticates the user at the RADIUS server.
  - *TACACS+* — Authenticates the user at the TACACS+ server.
  - *None* — Indicates that no authentication method is used to authenticate the user.

**STEP 2** Click the **Add** button. The *Add Authentication Profile Page* opens:



## Add Authentication Profile Page

## Add Authentication Profile

**Profile Name**

---

**Authentication Method**

Optional Methods

Local

RADIUS

TACACS+

>>

<<

Selected Methods

None

Apply

The *Add Authentication Profile Page* contains the following fields:

- **Profile Name** — Defines the Authentication profile name.
- **Authentication Method** — Defines the user authentication methods. The order of the authentication methods defines the order in which authentication is attempted. For example, if the authentication method order is RADIUS, Local, the system first attempts to authenticate the user on a RADIUS server. If there is no available RADIUS server, then authentication is attempted on the local data base. Note that if the RADIUS server is available, but authentication fails, then the user is denied access. The possible field values are:
  - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication. No option can be inserted below Local.
  - *RADIUS* — Authenticates the user at the RADIUS server.
  - *TACACS+* — Authenticates the user at the TACACS+ server.
  - *None* — Indicates that no authentication method is used to authenticate the user. No option can be inserted below None.

**STEP 3** Define the relevant fields.

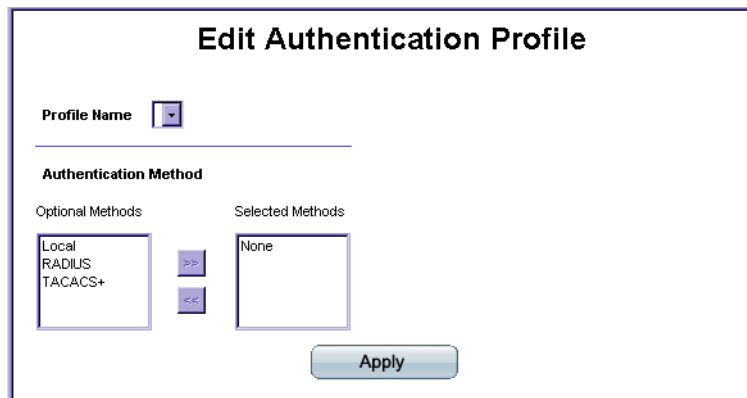
**STEP 4** Click **Apply**. The authentication profile is defined, the device is updated.

## Modifying an Authentication Profile

**STEP 1** Click **Security > Authentication > Profiles**. The *Profiles Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit Authentication Profile Page* opens:

### Edit Authentication Profile Page



The *Edit Authentication Profile Page* contains the following fields:

- **Profile Name** — Displays the Authentication profile name.
- **Authentication Methods** — Defines the user authentication methods. The possible field values are:
  - *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
  - *RADIUS* — Authenticates the user at the RADIUS server.
  - *TACACS+* — Authenticates the user at the TACACS+ server.
  - *None* — Indicates that no authentication method is used to authenticate the device.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The authentication profile is defined, the device is updated.

## Mapping Authentication Profiles

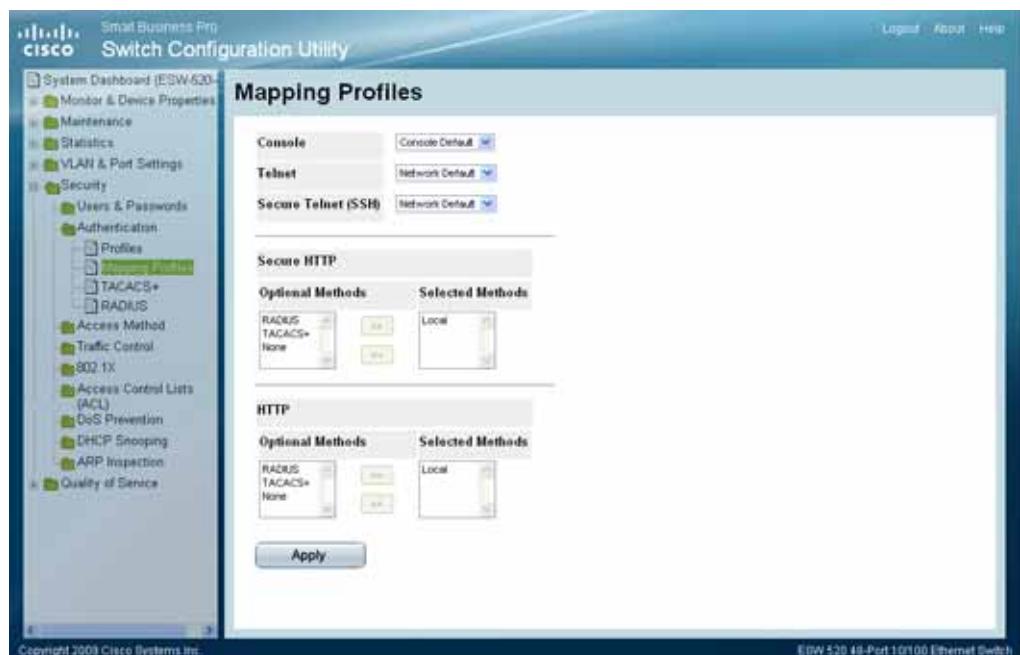
After authentication profiles are defined, authentication profiles can be applied to management access methods. For example, console users can be authenticated by one authentication profile, while Telnet users are authenticated by another authentication profile.

Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

The *Mapping Profiles Page* contains parameters for mapping authentication methods. To map authentication profiles:

- STEP 1** Click **Security > Authentication > Mapping Profiles**. The *Mapping Profiles Page* opens:

### Mapping Profiles Page



The *Mapping Profiles Page* contains the following fields:

- **Console** — Indicates that Authentication profiles are used to authenticate console users.
- **Telnet** — Indicates that Authentication profiles are used to authenticate Telnet users.

- **Secure Telnet (SSH)** — Indicates that Authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.

- **Secure HTTP** — Configures the device Secure HTTP settings.

*Optional Methods* — Lists available authentication methods.

- *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication. No authentication method can be added under Local.
- *RADIUS* — Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks.
- *TACACS+* — Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation.
- *None* — Indicates that no authentication method is used to authenticate the device. No authentication method can be added under None.

*Selected Methods* — Selects authentication methods from the methods offered in the Optional methods area.

- **HTTP** — Configures the device HTTP settings.

*Optional Methods* — Lists available authentication methods.

- *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication. No authentication method can be added under Local.
- *RADIUS* — Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks.
- *TACACS+* — Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation.
- *None* — Indicates that no authentication method is used to authenticate the device. No authentication method can be added under None.

*Selected Methods* — Selects authentication methods from the methods offered in the Optional methods area.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. Mapping Profiles is defined, and the device is updated.

## Defining TACACS+

The devices provide Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS server checks the user privileges.

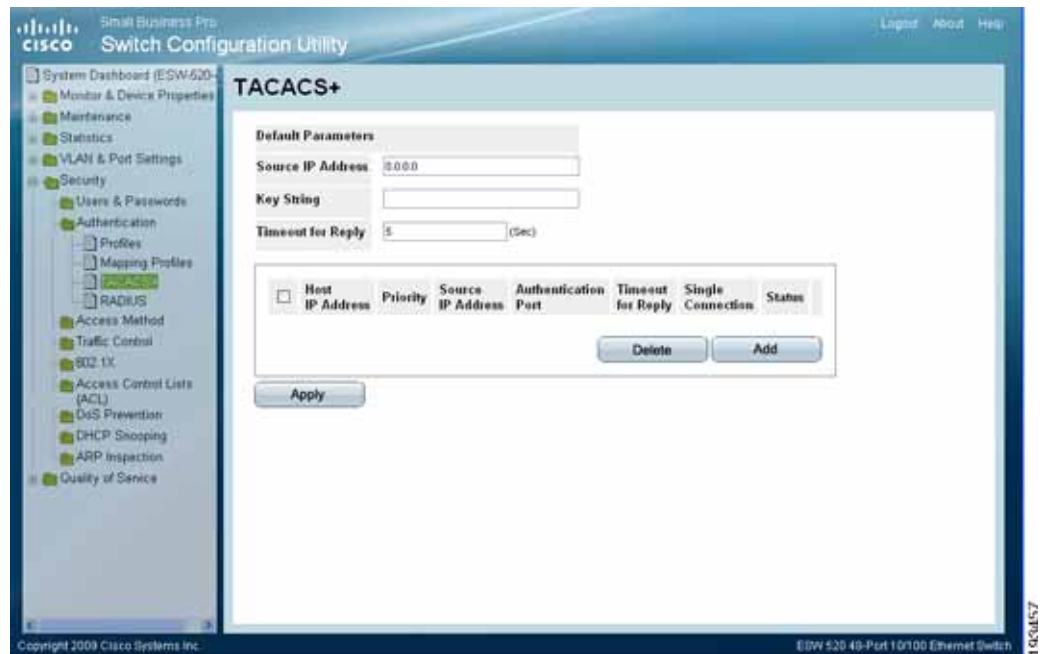
The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

The TACACS+ default parameters are user-assigned defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers. The *TACACS+ Page* contains fields for assigning the Default Parameters for the TACACS+ servers.

To define TACACS+:

**STEP 1** Click **Security > Authentication > TACACS+**. The *TACACS+ Page* opens:

#### TACACS+ Page



The *TACACS+ Page* contains the following fields:

- **Source IP Address** — Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- **Timeout for Reply** — Displays the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.

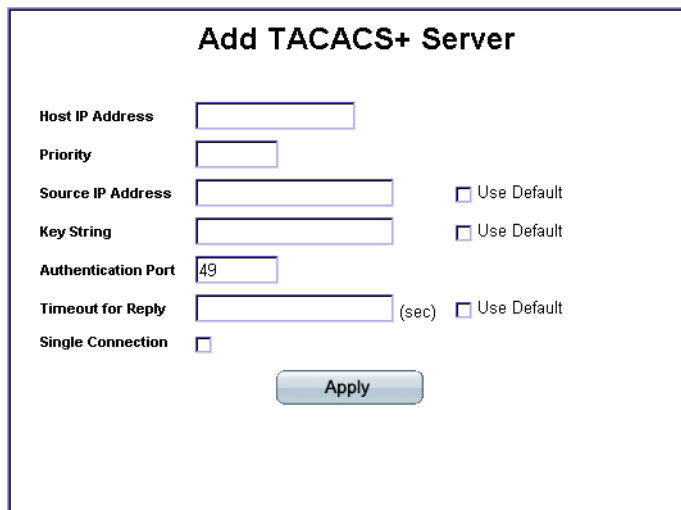
The following parameters are configured for each TACACS+ server:

- **Host IP Address** — Displays the TACACS+ Server IP address.
- **Priority** — Displays the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address** — Displays the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication Port** — Displays the port number through which the TACACS+ session occurs. The default is port 49.

- **Timeout for Reply** — Displays the amount of time in seconds that passes before the connection between the device and the TACACS+ times out. The field range is 1-1000 seconds.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server when selected.
- **Status** — Displays the connection status between the device and the TACACS+ server. The possible field values are:
  - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
  - *Not Connected* — Indicates there is no current connection between the device and the TACACS+ server.

**STEP 2** Click the **Add** button. The *Add TACACS+ Server Page* opens:

#### Add TACACS+ Server Page



The screenshot shows the 'Add TACACS+ Server' configuration page. It contains the following fields and options:

- Host IP Address**: A text input field.
- Priority**: A text input field.
- Source IP Address**: A text input field with a checkbox labeled 'Use Default' to its right.
- Key String**: A text input field with a checkbox labeled 'Use Default' to its right.
- Authentication Port**: A text input field containing the value '49'.
- Timeout for Reply**: A text input field with '(sec)' to its right and a checkbox labeled 'Use Default' to its right.
- Single Connection**: A checkbox.
- Apply**: A button at the bottom center.

The Add TACACS+ Server Page contains the following fields:

- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address** — Defines the device source address used for the TACACS+ session between the device and the TACACS+ server. The possible values are:
  - **User Defined** — Allows the user to define the source Address.

- **Use Default** — Uses the default value for the parameter. If Use Default check box is selected, the global value of 0.0.0.0. is used and interpreted as a request to use the IP address of the outgoing IP interface.
- **Key String** — Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server. The possible values are:
  - **User Defined** — Allows the user to define the Key String value.
  - **Use Default** — Uses the default value for the parameter. If Use Default check box is selected, the global value is used which is an empty string.
- **Authentication Port** — Defines the port number through which the TACACS+ session occurs. The default is port 49.
- **Timeout for Reply** — Defines the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
  - **User Defined** — Allows the user to define the Timeout for Reply value.
  - **Use Default** — Uses the default value for the parameter. If Use Default check box is selected, the default is 5 seconds.
- **Single Connection** — Enables a single open connection between the device and the TACACS+ server when selected.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The TACACS+ server is added, and the device is updated.

---

## Modifying TACACS+ Settings

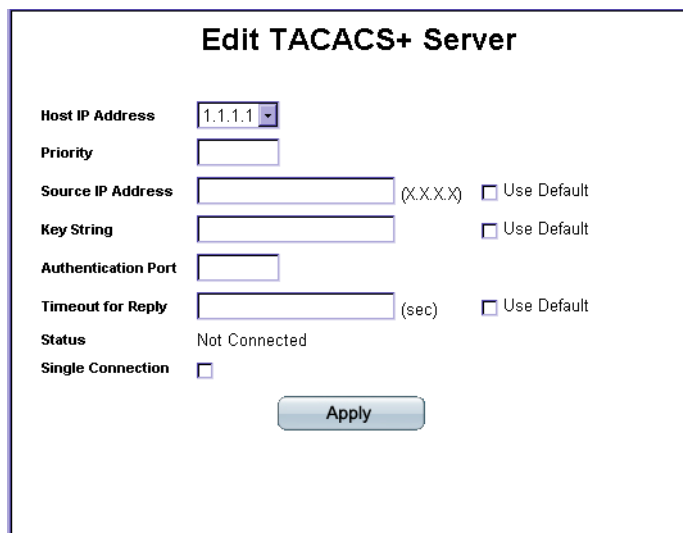
---

**STEP 1** Click **Security > Authentication > TACACS+**. The *TACACS+ Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit TACACS+ Server Page* opens:



#### Edit TACACS+ Server Page



The screenshot shows the 'Edit TACACS+ Server' configuration window. It contains the following fields and controls:

- Host IP Address:** A dropdown menu currently showing '1.1.1.1'.
- Priority:** An empty text input field.
- Source IP Address:** A text input field followed by '(X.X.X.X)' and a checkbox labeled 'Use Default'.
- Key String:** A text input field followed by a checkbox labeled 'Use Default'.
- Authentication Port:** A text input field.
- Timeout for Reply:** A text input field followed by '(sec)' and a checkbox labeled 'Use Default'.
- Status:** A label indicating 'Not Connected'.
- Single Connection:** A checkbox.
- Apply:** A button at the bottom right.

The *Edit TACACS+ Server Page* contains the following fields:

- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address** — Defines the device source address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String** — Defines the authentication and encryption key for TACACS+ server. The key must match the encryption key used on the TACACS+ server.
- **Authentication Port** — Defines the port number through which the TACACS+ session occurs. The default is port 49.
- **Timeout for Reply** — Defines the amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
- **Status** — Displays the connection status between the device and the TACACS+ server. The possible field values are:
  - *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
  - *Not Connected* — Indicates there is no current connection between the device and the TACACS+ server.

- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server when selected
- **Use Default** — Indicates that the factory default value is used.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The TACACS+ settings are modified, and the device is updated.

## Defining RADIUS

*Remote Authorization Dial-In User Service* (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access. The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

To define RADIUS:

**STEP 1** Click **Security > Authentication > RADIUS**. The *RADIUS Page* opens:

### RADIUS Page

The screenshot shows the 'RADIUS' configuration page within the 'Cisco Switch Configuration Utility'. The left sidebar contains a tree view with 'Security' expanded, showing 'Users & Passwords', 'Authentication', 'Profiles', 'Mapping Profiles', 'TACACS+', and 'RADIUS'. The 'RADIUS' section is selected. The main area is titled 'RADIUS' and contains the following fields:

- RADIUS Accounting**: A dropdown menu set to 'None'.
- Use Default Parameters**: A checkbox that is checked.
- Default Retries**: A text box containing the value '3'.
- Default Timeout for Reply**: A text box containing the value '3' with '(Sec)' to its right.
- Default Dead Time**: A text box containing the value '0' with '(Min)' to its right.
- Default Key String**: A text box.
- Source IP Address**: A text box containing the value '0.0.0.0'.

Below these fields is a table with the following columns: ☐ IP Address, Priority, Source IP Address, Authentication Port, Accounting Port, Number of Retries, Timeout for Reply, Dead Time, Key String, and Usage Type. There are 'Delete' and 'Add' buttons to the right of the table. At the bottom left of the main area is an 'Apply' button. The footer of the window shows 'Copyright 2009 Cisco Systems Inc.' and 'ESW 520 48-Port 10/100 Ethernet Switch'.

The *RADIUS Page* contains the following fields:

- **Radius Accounting** — Defines the authentication method used for RADIUS session accounting. Possible field values are:
  - *802.1x* — 802.1x authentication is used to initiate accounting.
  - *Login* — Login authentication is used to initiate accounting.
  - *Both* — Both 802.1x and login authentication are used to initiate accounting.
  - *None* — No authentication is used to initiate accounting.
- **Default Retries** — Provides the default retries.
- **Default Timeout for Reply** — Provides the device default Timeout for Reply.
- **Default Dead Time** — Provides the device default Dead Time.
- **Default Key String** — Provides the device default Default Key String.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.

The following parameters are configured for each RADIUS server:

- **IP Address** — Displays the Authentication Server IP addresses.
- **Priority** — Indicates the server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Source IP Address** — Displays the Authentication port's IP address.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authentication port default is 1812.
- **Accounting Port** — Indicates the port used to send login and logout messages to the RADIUS server. The accounting port default is 1813.
- **Number of Retries** — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply** — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.

- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:
  - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
  - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
  - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.

**STEP 2** Click the **Add** button. The *Add RADIUS Server Page* opens:

#### Add RADIUS Server Page

**Add RADIUS Server**

Host IP Address	<input type="text"/>	
Priority	<input type="text" value="0"/>	
Source IP Address	<input type="text" value="Default"/>	<input checked="" type="checkbox"/> Use Default
Authentication Port	<input type="text" value="1812"/>	
Accounting Port	<input type="text" value="1813"/>	
Number of Retries	<input type="text" value="Default"/>	<input checked="" type="checkbox"/> Use Default
Timeout for Reply	<input type="text" value="Default"/> (Sec)	<input checked="" type="checkbox"/> Use Default
Dead Time	<input type="text" value="Default"/> (Min)	<input checked="" type="checkbox"/> Use Default
Key String	<input type="text" value="Default"/> (Alphanumeric)	<input checked="" type="checkbox"/> Use Default
Usage Type	<input type="button" value="All"/>	

The *Add RADIUS Server Page* contains the following fields:

- **Host IP Address** — Displays the *RADIUS* Server IP address.

- **Priority** — Displays the server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authentication port default is 1812.
- **Accounting Port** — Indicates the port used to send login and logout messages to the RADIUS server. The accounting port default is 1813.
- **Number of Retries** — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply** — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:
  - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
  - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
  - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.
- **Use Default** — Uses the default value for the parameter.

#### STEP 3 Define the relevant fields.

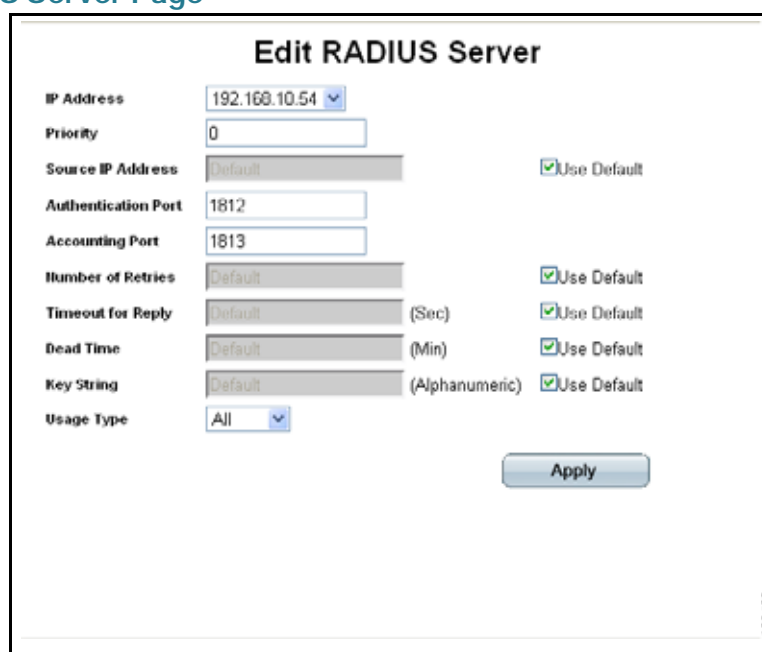
**STEP 4** Click **Apply**. The RADIUS Server is added, and the device is updated.

## Modifying RADIUS Server Settings

**STEP 1** Click **Security > Authentication > RADIUS**. The *RADIUS Page* opens:

**STEP 2** Click the **Edit** button. The *Edit RADIUS Server Page* opens:

### Edit RADIUS Server Page



The screenshot shows the 'Edit RADIUS Server' configuration page. It contains the following fields and options:

Field	Value	Unit/Type	Use Default
IP Address	192.168.10.54		
Priority	0		
Source IP Address	Default		<input checked="" type="checkbox"/>
Authentication Port	1812		
Accounting Port	1813		
Number of Retries	Default		<input checked="" type="checkbox"/>
Timeout for Reply	Default	(Sec)	<input checked="" type="checkbox"/>
Dead Time	Default	(Min)	<input checked="" type="checkbox"/>
Key String	Default	(Alphanumeric)	<input checked="" type="checkbox"/>
Usage Type	All		

An 'Apply' button is located at the bottom right of the form.

The *Edit RADIUS Server Page* contains the following fields:

- **IP Address** — Defines the RADIUS Server IP address.
- **Priority** — Displays the server priority. The possible values are 0-65535, where 1 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Authentication Port** — Displays the authentication port. The authentication port is used to verify the RADIUS server authentication. The authentication port default is 1812.

- **Accounting Port** — Indicates the port used to send login and logout messages to the RADIUS server. The accounting port default is 1813.
- **Number of Retries** — Defines the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. Three is the default value.
- **Timeout for Reply** — Defines the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The Dead Time default is 0 minutes.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is Login. The possible field values are:
  - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
  - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
  - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.
- **Use Default** — Uses the default value for the parameter.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The RADIUS Server is modified, and the device is updated.

---

## Defining Access Methods

The access method section contains the following pages:

- Defining Access Profiles

- Defining Profile Rules

## Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP
- Secure HTTP (HTTPS)
- SNMP

Management access to different management methods may differ between user groups. For example, User Group 1 can access the switch module only via an HTTPS session, while User Group 2 can access the switch module via both HTTPS and Telnet sessions. The Access Profile Page contains the currently configured access profiles and their activity status. Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces.

To define access profiles:



- STEP 1** Click **Security > Access Method > Access Profiles**. The *Access Profiles Page* opens:

#### Access Profiles Page



The *Access Profiles Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Current Active Access Profile** — Defines the access profile currently active.

- STEP 2** Click the **Add** button. The *Add Access Profile Page* opens:

#### Add Access Profile Page

**Add Access Profile**

Access Profile Name

---

Rule Priority

Management Method

☐ Interface ☐ Port  ☐ EtherChannel  ☐ VLAN

☐ Source IP Address  ☐ Network Mask  ☐ Prefix Length

Action

Cisco ISE

The Add Access Profile Page contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.

- *HTTP*— Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (HTTPS)*— Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *SNMP*— Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  - *Port*— Specifies the port on which the access profile is defined.
  - *EtherChannel*— Specifies the EtherChannel on which the access profile is defined.
  - *VLAN*— Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- **Network Mask** — Determines what subnet the source IP Address belongs to in the network.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
  - *Permit*— Permits access to the device.
  - *Deny*— Denies access to the device. This is the default.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The access profile is added, and the device is updated.

---

## Defining Profile Rules

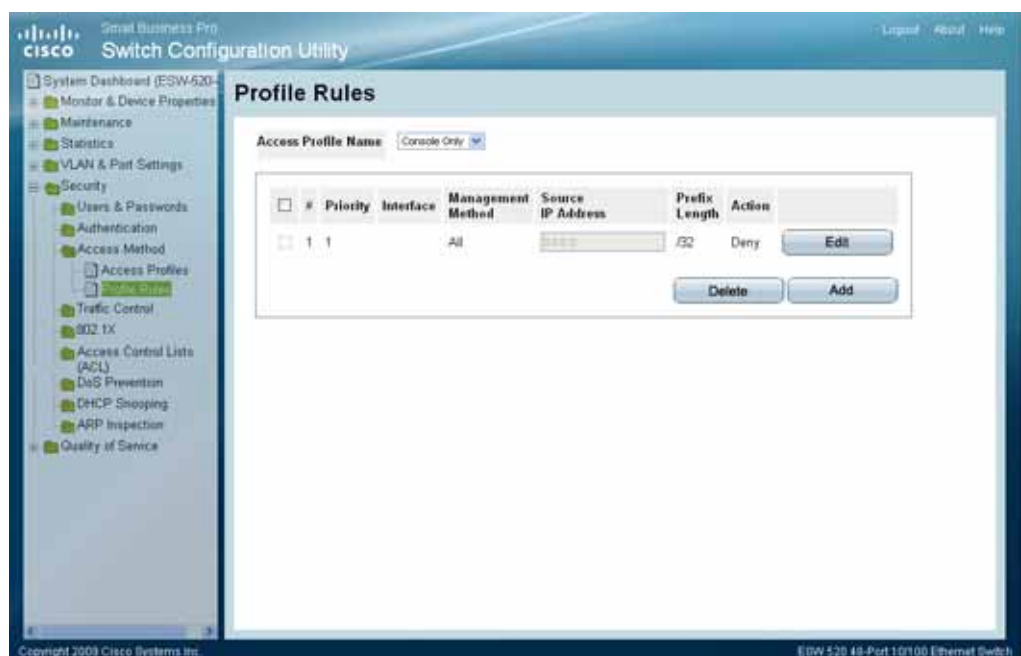
Access profiles can contain up to 128 rules that determine which users can manage the switch module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- IP Address
- Prefix Length
- Forwarding Action

To define profile rules:

**STEP 1** Click **Security > Access Method > Profile Rules**. The *Profile Rules Page* opens:

#### Profile Rules Page



The *Profile Rules Page* contains the following fields:

- **Access Profile Name** — Displays the access profile to which the rule is attached.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.

- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
  - *Port* — Attaches the rule to the selected port.
  - *EtherChannel* — Attaches the rule to the selected EtherChannel.
  - *VLAN* — Attaches the rule to the selected VLAN.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
  - *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (SSL)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- **Source IP Address** — Defines the interface source IP address to which the rule applies.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

**STEP 2** Click the **Add** button. The *Add Profile Rule Page* opens:

#### Add Profile Rule Page

The *Add Profile Rule Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.

- *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (SSL)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  - *Port* — Specifies the port on which the access profile is defined.
  - *EtherChannel* — Specifies the EtherChannel on which the access profile is defined.
  - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- **Network Mask** — Determines what subnet the source IP Address belongs to in the network.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The profile rule is added, and the device is updated.

---

## Modifying Profile Rules

---

**STEP 1** Click **Security > Access Method > Profile Rules**. The *Profile Rules Page* opens:

**STEP 2** Click the **Edit** button. The *Edit Profile Rule Page* opens:

#### Edit Profile Rule Page

The screenshot shows the 'Edit Profile Rule' configuration page. At the top, the title 'Edit Profile Rule' is centered. Below it, the 'Access Profile Name' is set to 'Default'. The 'Priority' is a text input field containing the number '3'. The 'Management Method' is a dropdown menu currently showing 'All'. Below this, there are three radio button options: 'Interface', 'Port', and 'EtherChannel'. The 'Interface' option is selected. Under 'Interface', there are two sub-options: 'Port' (with a dropdown showing 'e1') and 'EtherChannel' (with a dropdown showing '1'). The 'Port' option is selected. Below these, there are two radio button options: 'Network Mask' and 'Prefix Length'. The 'Network Mask' option is selected, and its value is '255.255.255.255'. The 'Prefix Length' option is unselected, and its value is '/32'. The 'Action' is a dropdown menu currently showing 'Permit'. At the bottom center, there is an 'Apply' button. In the bottom right corner, there is a small vertical text label '130467'.

The *Edit Profile Rule Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Page.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  - *All* — Assigns all management methods to the rule.
  - *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  - *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.



- *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  - *Secure HTTP (SSL)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  - *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  - *Port* — Specifies the port on which the access profile is defined.
  - *EtherChannel* — Specifies the EtherChannel on which the access profile is defined.
  - *VLAN* — Specifies the VLAN on which the access profile is defined.
- **Source IP Address** — Defines the interface source IP address to which the access profile applies. The Source IP Address field is valid for a subnetwork.
- **Network Mask** — Determines what subnet the source IP Address belongs to in the network.
- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
  - *Permit* — Permits access to the device.
  - *Deny* — Denies access to the device. This is the default.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The profile rules are defined, and the device is updated.

## Defining Traffic Control

The Traffic Control section contains the following pages:

- Defining Storm Control
- Defining Port Security

## Defining Storm Control

Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected on all ports.

A Broadcast Storm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

Storm Control is enabled per all ports by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast and Multicast frame rates separately on each port and discards the frames when the rate exceeds a user-defined rate.



### NOTE

Storm Control is enabled per port on GE devices, and per system on FE devices (not applicable to ESW 520-8P devices).

The *Storm Control Page* provides fields for configuring Broadcast Storm Control.

To define storm control:

**STEP 1** Click **Security > Traffic Control > Storm Control**. The *Storm Control Page* opens:

#### Storm Control Page

#	Port	Enable Broadcast Control	Broadcast Rate Threshold	Broadcast Mode	
1	e1	Enabled	10000	Broadcast Only	Edit
2	e2	Enabled	10000	Broadcast Only	Edit
3	e3	Enabled	10000	Broadcast Only	Edit
4	e4	Enabled	10000	Broadcast Only	Edit
5	e5	Enabled	10000	Broadcast Only	Edit
6	e6	Enabled	10000	Broadcast Only	Edit
7	e7	Enabled	10000	Broadcast Only	Edit
8	e8	Enabled	10000	Broadcast Only	Edit
9	e9	Enabled	10000	Broadcast Only	Edit

The *Storm Control Page* contains the following fields:

- **Unknown Unicast Group Control** — On ESW 520 devices, sets the Unknown Unicast Control as the Broadcast Mode globally defined on the device.
- **Rate Threshold** — On FE devices, sets the maximum rate (packets per second) at which unknown packets are forwarded. The range rate is 3500-100,000 Kbps.
- **Copy From Entry Number** — Copies the storm control configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied storm control configuration to the specified table entry.
- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — Indicates if Broadcast packet types are forwarded on the specific interface. The possible field values are:
  - *Enable* — Enables Broadcast packet types to be forwarded. This is the default value.

- *Disable* — Disables Broadcast packet types to be forwarded.
- **Broadcast Rate Threshold** — Indicates the maximum rate (kilobits per second) at which unknown packets are forwarded.
  - For FE ports, the rate is 70 - 100,000 Kbps.
  - For GE ports, the rate is 3,500 - 100,000 Kbps.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field values are:
  - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
  - *Broadcast Only* — Counts only Broadcast traffic.
  - *Unknown Unicast* — Counts only Unknown Unicast. Relevant on ESW 540, ESW 520, and ESW 520-8p devices.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. Storm control is enabled, and the device is updated.

---

## Modifying Storm Control

**STEP 1** Click **Security > Traffic Control > Storm Control**. The *Storm Control Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit Storm Control Page* opens:

### Edit Storm Control Page



The screenshot shows the 'Edit Storm Control' configuration page. It contains the following fields and controls:

- Port:** A dropdown menu with 'g1' selected.
- Enable Broadcast Control:** A checkbox that is checked.
- Broadcast Mode:** A dropdown menu with 'Broadcast Only' selected.
- Broadcast Rate Threshold:** A text input field containing '10000', followed by the unit '(Kbits/sec)'.
- Apply:** A button located at the bottom right of the form.

The *Edit Storm Control Page* contains the following fields:

- **Port** — Indicates the port from which storm control is enabled.
- **Enable Broadcast Control** — Indicates if Broadcast packet types are forwarded on the specific interface. The possible field values are:
  - *Checked* — Enables Broadcast packet types to be forwarded.
  - *Unchecked* — Disables Broadcast packet types to be forwarded.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the interface. The possible field values are:
  - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
  - *Broadcast Only* — Counts only Broadcast traffic.
  - *Unknown Unicast, Multicast & Broadcast* — Counts Unknown Unicast, Broadcast and Multicast traffic together. This option is available on GE ports only. On FE devices, this option can only be set globally for the device from the *Storm Control Page*. Relevant on ESW-540, ESW-520, and ESW-520-8p devices.
- **Broadcast Rate Threshold** — Displays the maximum rate (packets per second) at which unknown packets are forwarded.
  - For FE ports, the rate is 70 - 100,000 Kbps.
  - For GE ports, the rate is 3,500 - 100,000 Kbps.

**STEP 3** Modify the relevant fields.

**STEP 4** Click **Apply**. Storm control is modified, and the device is updated.

---

## Defining Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned or statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is

locked. When a packet is received on a locked port, and the packet source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving at a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- Cause the port to be shut down.

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset. Disabled ports are activated from the Port Security Page.



---

**NOTE** To configure port lock, 802.1x multiple host mode must be enabled.

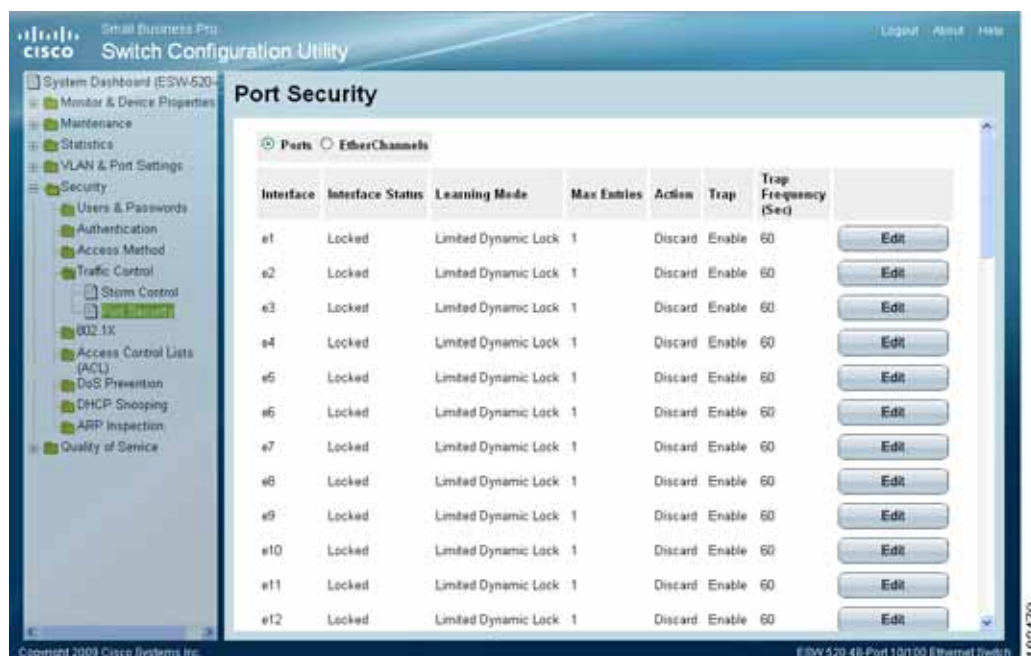
---

To define port security:

**STEP 1** Click **Security > Traffic Control > Port Security**. The *Port Security Page* opens:

### Port Security Page

The *Port Security Page* contains the following fields:



- **Ports Radio Button** — Indicates the Port on which port security is configured.
- **EtherChannels Radio Button** — Indicates the EtherChannel on which port security is configured.
- **Interface** — Displays the port or EtherChannel name.
- **Interface Status** — Indicates the port security status. The possible field values are:
  - *Unlocked* — Indicates the port is currently unlocked. This is the default value.
  - *Locked* — Indicates the port is currently locked.
- **Learning Mode** — Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated. The possible field values are:

- *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
- *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.



**NOTE** For the port transitioning from classic lock to limited dynamic lock, previously learned MAC addresses are not deleted but are converted to a static MAC address.

- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The possible range is 1-128. The default is 1.
- **Action** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
  - *Forward* — Forwards packets from an unknown source without learning the MAC address.
  - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
  - *Enable* — Enables traps.
  - *Disable* — Disables traps.
- **Trap Frequency (Sec)** — Displays the amount of time (in seconds) between traps. The default value is 10 seconds.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. Port security is defined, and the device is updated.

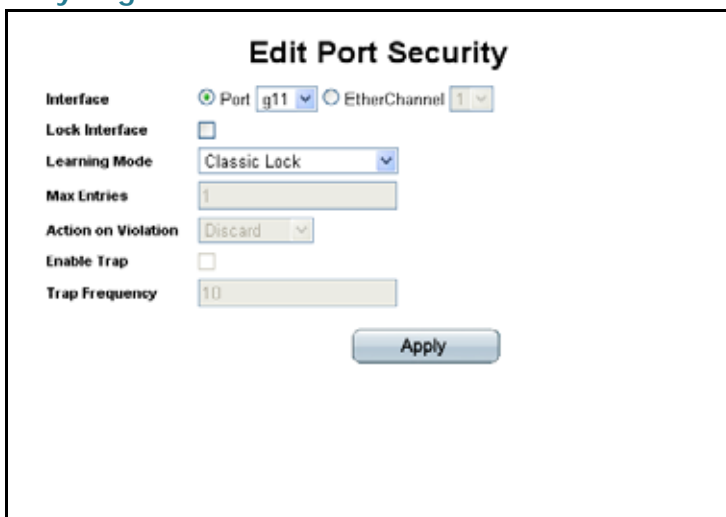


## Modifying Port Security

**STEP 1** Click **Security > Traffic Control > Port Security**. The *Port Security Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit Port Security Page* opens:

### Edit Port Security Page



The screenshot shows the 'Edit Port Security' configuration page. It contains the following fields and controls:

- Interface:** Radio buttons for 'Port' (selected) and 'EtherChannel'. The 'Port' dropdown is set to 'g11' and the 'EtherChannel' dropdown is set to '1'.
- Lock Interface:** An unchecked checkbox.
- Learning Mode:** A dropdown menu set to 'Classic Lock'.
- Max Entries:** A text input field containing the value '1'.
- Action on Violation:** A dropdown menu set to 'Discard'.
- Enable Trap:** An unchecked checkbox.
- Trap Frequency:** A text input field containing the value '10'.
- Apply:** A button at the bottom right.

The *Edit Port Security Page* contains the following fields:

- **Interface** — Select the port or EtherChannel name.
- **Lock Interface** — Indicates the port security status. The possible field values are:
  - *Unchecked* — Indicates the port is currently unlocked. This is the default value.
  - *Checked* — Indicates the port is currently locked.
- **Learning Mode** — Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Interface Status field. In order to change the Learning Mode, the Lock Interface must be set to Unlocked. Once the mode is changed, the Lock Interface can be reinstated. The possible field values are:
  - *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
  - *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the

maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled. Previously learned MAC addresses are not deleted but are converted to a static MAC address.

- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Interface Status field. In addition, the Limited Dynamic Lock mode is selected. The possible range is 1-128. The default is 1.
- **Action on Violation** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
  - *Discard* — Discards packets from any unlearned source. This is the default value.
  - *Forward* — Forwards packets from an unknown source without learning the MAC address.
  - *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Enable Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
  - *Checked* — Enables traps.
  - *Unchecked* — Disables traps.
- **Trap Frequency** — Displays the amount of time (in seconds) between traps. The default value is 10 seconds.

**STEP 3** Modify the relevant fields.

**STEP 4** Click **Apply**. Port security is modified, and the device is updated.

## Defining 802.1x

Port based authentication enables authenticating system users on a per-port basis via a external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP). Port Authentication includes:

- **Authenticators** — Specifies the port, which is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The 802.1x section contains the following pages:

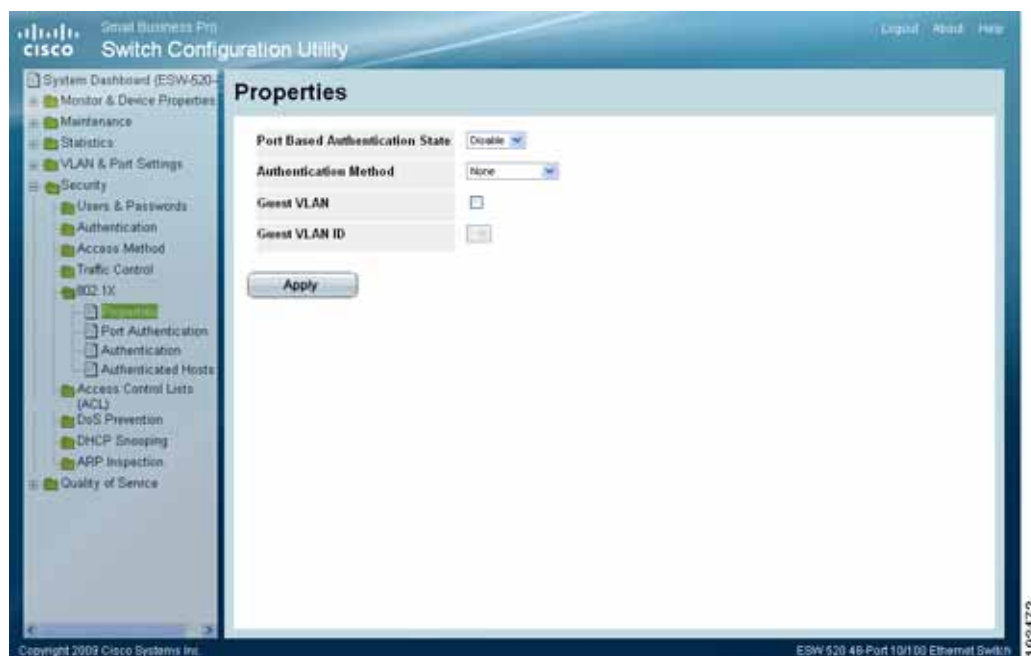
- Defining 802.1X Properties
- Defining Port Authentication
- Defining Authentication
- Defining Authenticated Host

## Defining 802.1X Properties

The 802.1X Properties Page provides parameters for enabling port authentication, and selecting the authentication method. To define port based authentication:

**STEP 1** Click **Security > 802.1X > Properties**. The *802.1X Properties Page* opens:

#### 802.1X Properties Page



The *802.1X Properties Page* contains the following fields:

- **Port Based Authentication State** — Enables Port-based Authentication on the device. The possible field values are:
  - *Enable* — Enables port-based authentication on the device.
  - *Disable* — Disables port-based authentication on the device.
- **Authentication Method** — Defines the user authentication methods. The possible field values are:
  - *RADIUS, None* — Indicates port authentication is performed first via the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then the *None* option is used, and the session is permitted.
  - *RADIUS* — Authenticates the user at the RADIUS server.
  - *None* — No authentication method is used to authenticate the port.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:

- *Checked*— Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
- *Unchecked*— Disables use of a Guest VLAN for unauthorized ports. This is the default.
- **Guest VLAN ID** — Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The 802.1X properties are defined, and the device is updated.

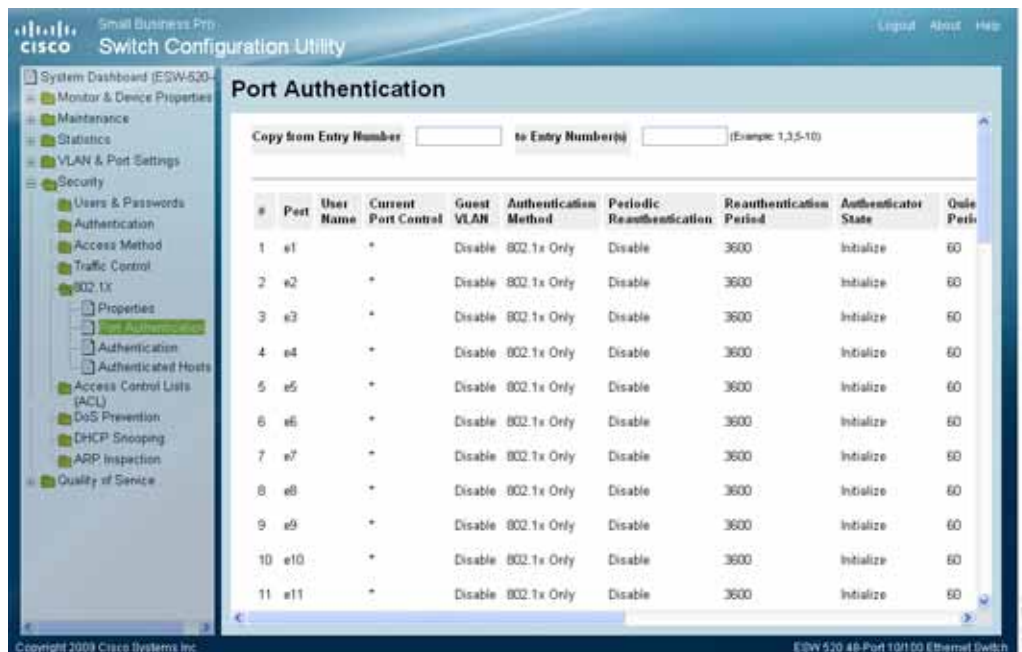
---

## Defining Port Authentication

The *802.1X Port Authentication Page* provides parameters for defining 802.1X on ports.

- STEP 1** Click **Security > 802.1X > Port Authentication**. The *802.1X Port Authentication Page* opens:

#### 802.1X Port Authentication Page



The *802.1X Port Authentication Page* contains the following fields:

- **Copy From Entry Number** — Copies the port authentication configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied port authentication configuration to the specified table entry.
- **Port** — Displays the list of interfaces.
- **User Name** — Displays the user name.
- **Current Port Control** — Displays the current port authorization state.
- **Guest VLAN** — Displays the Guest VLAN.
- **Authentication Method** — Displays the authentication method in use. The possible field values are:
  - *802.1x Only* — Enables only 802.1x authentication on the device.
  - *MAC Only* — Enables only MAC Authentication on the device.

- **802.1x & MAC** — Enables 802.1x + MAC Authentication on the device. In the case of 802.1x + MAC, 802.1x takes precedence.
- **Periodic Reauthentication** — Enables port reauthentication. The default value is disabled.
- **Reauthentication Period** — Specifies the number of seconds in which the selected port is reauthenticated (Range: 300-4294967295). The field default is 3600 seconds.
- **Authenticator State** — Specifies the port authorization state. The possible field values are as follows:
  - *Force-Authorized* — Indicates the controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized* — Indicates the controlled port state is set to Force-Unauthorized (discard traffic).
  - *Initialize* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
- **Quiet Period** — Specifies the number of seconds that the switch remains in the quiet state following a failed authentication exchange (Range: 0-65535).
- **Resending EAP** — Specifies the number of seconds that the switch waits for a response to an EAP - request/identity frame, from the supplicant (client), before resending the request.
- **Max EAP Requests** — Indicates the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the number of seconds that lapses before EAP requests are resent to the supplicant (Range: 1-65535). The field default is 30 seconds.
- **Server Timeout** — Specifies the number of seconds that lapses before the switch resends a request to the authentication server (Range: 1-65535). The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

#### STEP 2 Define the relevant fields

- STEP 3** Click **Apply**. The 802.1X port authentication settings are defined, and the device is updated.

## Modifying 8021X Security

- STEP 1** Click **Security > 802.1X > Port Authentication**. The *802.1X Properties Page* opens:

- STEP 2** Click the **Edit** button. The *Port Authentication Settings Page* opens:

### Port Authentication Settings Page

**Port Authentication Settings**

Port	<input type="text"/>
User Name	<input type="text"/>
Current Port Control	Authorized
Admin Port Control	forceAuthorized
Enable Guest VLAN	<input type="checkbox"/>
Authentication Method	802.1x Only
Enable Periodic Reauthentication	<input type="checkbox"/>
Reauthentication Period	3600
Reauthenticate Now	<input type="checkbox"/>
Authenticator State	Force Authorized
Quiet Period	60 (Sec)
Resending EAP	30 (Sec)
Max EAP Requests	2 (Sec)
Supplicant Timeout	30 (Sec)
Server Timeout	30 (Sec)
Termination Cause	Not terminated yet

**Apply**

The *Port Authentication Settings Page* contains the following fields:

- **Port** — Indicates the port on which port-based authentication is enabled.
- **User Name** — Displays the user name.
- **Current Port Control** — Displays the current port authorization state.
- **Admin Port Control** — Defines the admin port authorization state. The possible field values are:



- *auto* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - *forceAuthorized* — Indicates the interface is in an authorized state without being authenticated. The interface re-sends and receives normal traffic without client port-based authentication.
  - *forceUnauthorized* — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.
- **Enable Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  - *Checked* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the *VLAN List* field.
  - *Unchecked* — Disables port-based authentication on the device. This is the default.
- **Authentication Method** — Defines the user authentication method. The possible field values are:
  - *802.1x Only* — Enables only 802.1x authentication on the device.
  - *MAC Only* — Enables only MAC Authentication on the device.
  - *802.1x & MAC* — Enables 802.1x + MAC Authentication on the device. In the case of 802.1x + MAC, 802.1x takes precedence.
- **Enable Periodic Reauthentication** — Permits port reauthentication during the specified Reauthentication Period (see below). The possible field values are:
  - *Checked* — Enables immediate port reauthentication. This is the default value.
  - *Unchecked* — Disables port reauthentication.
- **Reauthentication Period** — Specifies the number of seconds in which the selected port is reauthenticated (Range: 300-4294967295). The field default is 3600 seconds.
- **Reauthenticate Now** — Specifies that authentication is applied on the device when the **Apply** button is pressed.
  - *Checked* — Enables immediate port reauthentication.

- *Unchecked* — Port authentication according to the Reauthentication settings above.
- **Authenticator State** — Specifies the port authorization state. The possible field values are as follows:
  - *Initialize* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  - *Force-Authorized* — Indicates the controlled port state is set to Force-Authorized (forward traffic).
  - *Force-Unauthorized* — Indicates the controlled port state is set to Force-Unauthorized (discard traffic).
- **Quiet Period** — Specifies the number of seconds that the switch remains in the quiet state following a failed authentication exchange (Range: 0-65535).
- **Resending EAP** — Specifies the number of seconds that the switch waits for a response to an EAP - request/identity frame, from the supplicant (client), before resending the request.
- **Max EAP Requests** — Displays the total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.
- **Supplicant Timeout** — Displays the number of seconds that lapses before EAP requests are resent to the supplicant (Range: 1-65535). The field default is 30 seconds.
- **Server Timeout** — Specifies the number of seconds that lapses before the switch resends a request to the authentication server (Range: 1-65535). The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated, if applicable.

**STEP 3** Modify the relevant fields.

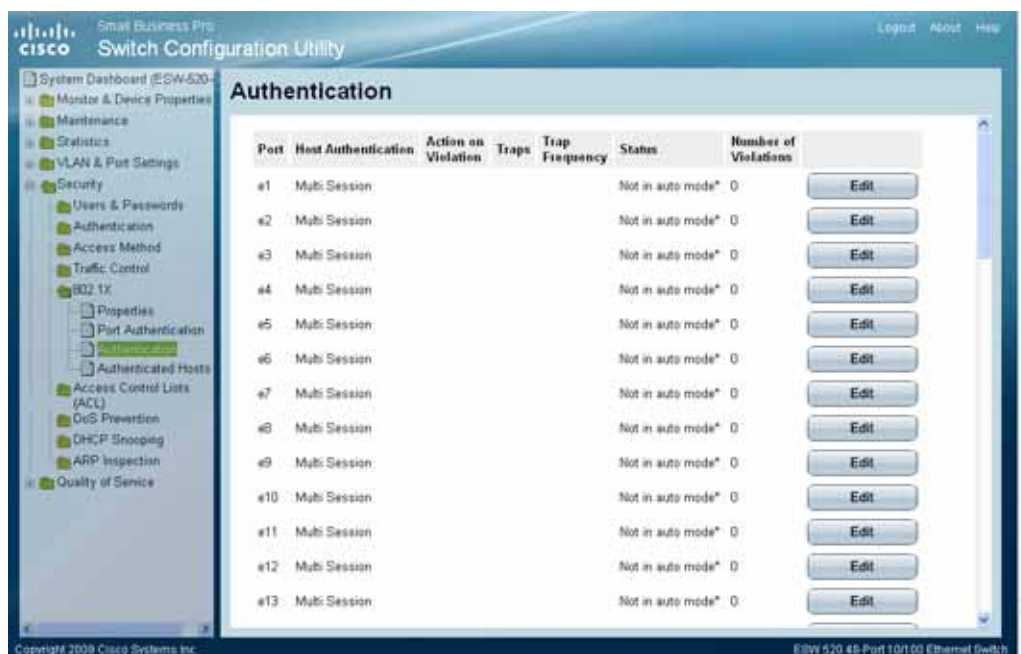
**STEP 4** Click **Apply**. The port authentication settings are defined, and the device is updated.

## Defining Authentication

The *802.1X Authentication Page* allows network managers to configure advanced port-based authentication settings for specific ports and VLANs.

**STEP 1** Click **Security > 802.1X > Authentication**. The *802.1X Authentication Page* opens:

### 802.1X Authentication Page



The *802.1X Authentication Page* contains the following fields:

- **Port** — Displays the port number for which the Multiple Hosts configuration is displayed.
- **Host Authentication**— Defines the Host Authentication mode. The possible field values are:
  - *Single* — Only the authorized host can access the port.
  - *Multiple Host* — Multiple hosts can be attached to a single 802.1x-enabled port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
  - *Multi Session* — Enables number of specific authorized hosts to get access to the port. Filtering is based on the source MAC address.

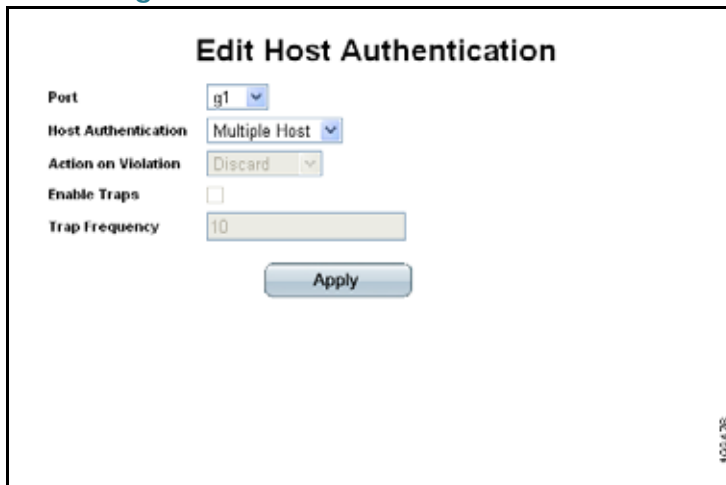
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - *Forward* — Forwards the packet.
  - *Discard* — Discards the packets. This is the default value.
  - *Shut Down* — Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- **Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
  - *Enable* — Indicates that traps are enabled for Multiple hosts.
  - *Disable* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- **Status** — Indicates the host status. If there is an asterisk \*, the port is either not linked or is down. The possible field values are:
  - *Not in Auto Mode* — Indicates the port is not linked or is down.
  - *Unauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port.
  - *Force-Authorized* — Indicates that the port control is Forced Authorized, and clients have full port access.
  - *Single-host Lock* — Indicates that the port control is Auto and only a single client has been authenticated via the port.
  - *Multiple Hosts* — Indicates that the port control is Auto and Multiple Hosts mode is enabled. One client has been authenticated.
  - *Multiple Sessions* — Indicates that the port control is Auto and Multiple Sessions mode is enabled. At least one client has been authenticated.
- **Number of Violations** — Indicates the number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

## Modifying Authentication Settings

**STEP 1** Click **Security > 802.1X > Authentication**. The *802.1X Port Authentication Page* opens:

**STEP 2** Click the **Edit** button. The *Edit Authentication Page* opens:

### Edit Authentication Page



The *Edit Authentication Page* contains the following fields:

- **Port** — Displays the port number for which advanced port-based authentication is enabled.
- **Host Authentication** — Defines the Host Authentication mode. The possible field values are:
  - *Single* — Only the authorized host can access the port.
  - *Multiple Host* — Multiple hosts can be attached to a single 802.1x-enabled port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
  - *Multi Session* — Enables number of specific authorized hosts to get access to the port. Filtering is based on the source MAC address.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - *Forward* — Forwards the packet.

- *Discard* — Discards the packets. This is the default value.
  - *Shut Down* — Discards the packets and shuts down the port. The ports remains shut down until reactivated, or until the device is reset.
- **Enable Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
  - *Checked* — Indicates that traps are enabled for Multiple hosts.
  - *Unchecked* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.

**STEP 3** Modify the relevant fields.

**STEP 4** Click **Apply**. The authentication settings are defined, and the device is updated.

---

## Authenticated Hosts

The *Authenticated Hosts Page* contains a list of authenticated users.

- STEP 1** Click **Security > 802.1X > Authenticated Hosts**. The *Authenticated Host Page* opens:

#### Authenticated Hosts Page



The *Authenticated Hosts Page* contains the following fields:

- **User Name** — Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** — Displays the port number.
- **Session time** — Displays the amount of time (in seconds) the supplicant was logged on the port.
- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
  - *Remote* — Indicates the 802.1x authentication is not used on this port (port is forced-authorized).
  - *None* — Indicates the supplicant was not authenticated.

- **RADIUS** — Indicates the supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

## Defining Access Control

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Your switch supports up to 256 ACLs. Packets entering an ingress port, with an active ACL, are either admitted or denied entry. If they are denied entry, the user can disable the port. ACLs are composed of Access Control Entries (ACEs) that are made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 256.

The Access Control section contains the following pages:

- Defining MAC Based ACL
- Defining IP Based ACL
- Defining ACL Binding

### Defining MAC Based ACL

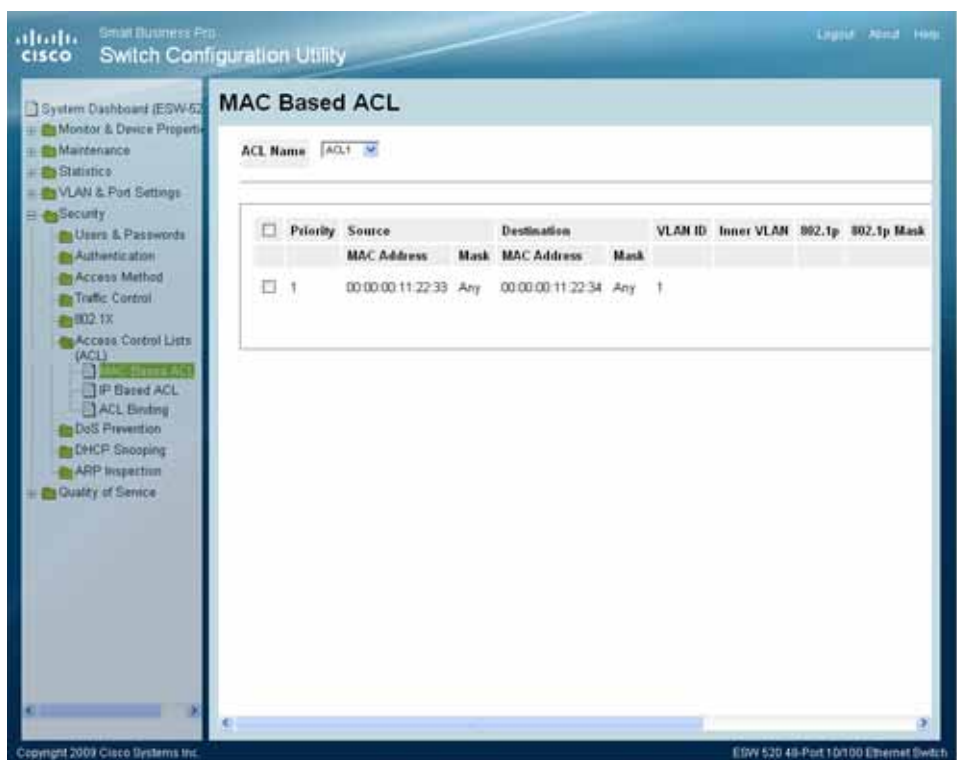
The *MAC Based ACL Page* allows a MAC-based Access Control List (ACL) to be defined. The table lists Access Control Elements (ACE) rules, which can be added only if the ACL is not bound to an interface.

To define the MAC Based ACL:

- STEP 1** Click **Security > Access Control Lists (ACL) > MAC Based ACL**. The *MAC Based ACL Page* opens:



#### MAC Based ACL Page



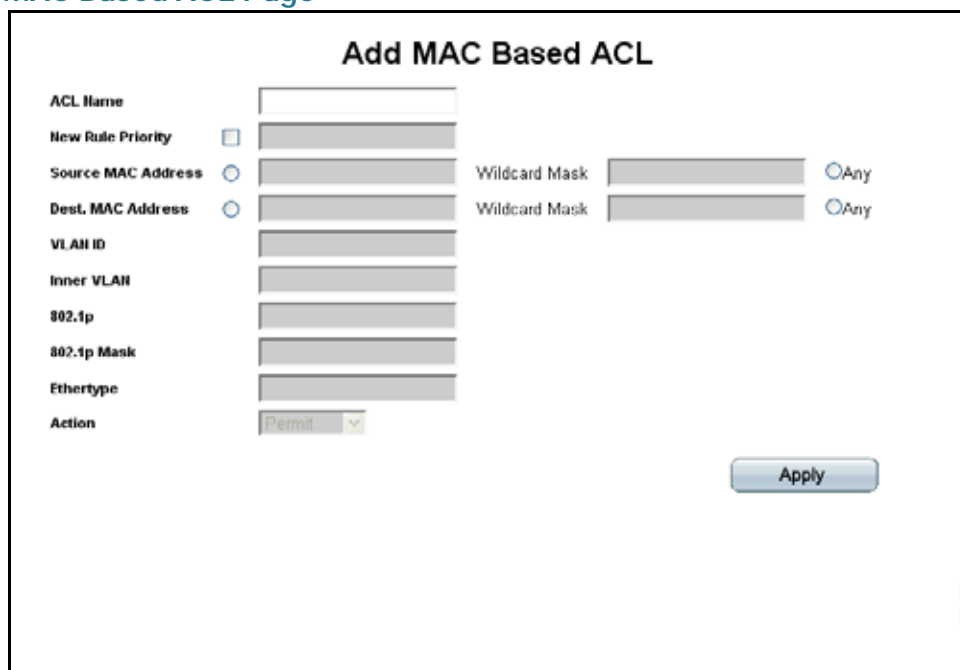
The *MAC Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address** — Defines the source MAC address to match the ACE.
- **Source MAC Mask** — Defines the source MAC mask to match the ACE.
- **Destination MAC Address** — Defines the destination MAC address to match the ACE.
- **Destination MAC Mask** — Defines the destination MAC mask to the which packets are matched.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4093.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.

- **802.1p Mask** — Displays the wildcard bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. For example, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. Possible field values are:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the Edit Interface Settings Page.

**STEP 2** Click the **Add ACL** button. The *Add MAC Based ACL Page* opens:

#### Add MAC Based ACL Page



The *Add MAC Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **New Rule Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address:**

- *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.
  - *Wildcard Mask* — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **Destination MAC Address:**
  - *MAC Address* — Matches the destination MAC address to which packets are addressed to the ACE.
  - *Wildcard Mask* — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination IP address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcards bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. The possible field values are:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The MAC Based ACL is defined, and the device is updated.

### Adding Rule to MAC Based ACL

**STEP 1** Click **Security > Access Control Lists (ACL) > MAC Based ACL**. The *MAC Based ACL* Page opens.

**STEP 2** Select an existing ACL from the *ACL Name* drop-down list.

**STEP 3** Click the **Add Rule** button. The *Add Rule Page* opens:

#### Add MAC Based Rule Page

The *Add MAC Based Rule Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **New Rule Priority** — Indicates the ACE priority, which determines which ACE is matched to a packet on a first-match basis. The possible field values are 1-2147483647.
- **Source MAC Address**

- *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.
  - *Wildcard Mask* — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **Destination MAC Address**
  - *MAC Address* — Matches the destination MAC address to which packets are addressed to the ACE.
  - *Wildcard Mask* — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination IP address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcard bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. The possible field values are:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

**STEP 4** Define the relevant fields.

**STEP 5** Click **Apply**. The ACL Rule is defined, and the device is updated.

### Modifying MAC Based ACL

**STEP 1** Click **Security > Access Control Lists (ACL) > MAC Based ACL**. The *MAC Based ACL Page* opens.

**STEP 2** Click the **Edit** button. The *Rule Settings Page* opens:

#### Rule Settings Page

The screenshot shows the 'Rule Settings' page for a MAC Based ACL. The page has a title 'Rule Settings' at the top center. Below the title, there are several fields for configuration. On the left side, there is a list of fields: 'ACL Name', 'Rule Priority', 'Source MAC Address', 'Dest. MAC Address', 'VLAN ID', 'Inner VLAN', '802.1p', '802.1p Mask', 'Ethertype', and 'Action'. The 'ACL Name' field is filled with 'ACL1'. The 'Rule Priority' field is filled with '1'. The 'Source MAC Address' field is filled with '00:00:00:11:22:33' and has a green circular icon with a plus sign to its left. The 'Dest. MAC Address' field is filled with '00:00:00:11:22:34' and has a green circular icon with a plus sign to its left. The 'VLAN ID' field is filled with '1'. The 'Inner VLAN' field is empty. The '802.1p' field is empty. The '802.1p Mask' field is empty. The 'Ethertype' field is empty. The 'Action' field is a dropdown menu with 'Permit' selected. On the right side, there are two 'Wildcard Mask' fields, both empty, each with a radio button labeled 'Any' to its right. At the bottom right of the page, there is an 'Apply' button.

The *Rule Settings Page* contains the following fields:

- **ACL Name** — Displays the user-defined MAC based ACLs.
- **Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Source MAC Address:**
  - *MAC Address* — Matches the source MAC address from which packets are addressed to the ACE.

- *Wildcard Mask* — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **Destination MAC Address:**
  - *MAC Address* — Matches the destination MAC address to which packets are addressed to the ACE.
  - *Wildcard Mask* — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination IP address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Inner VLAN** — Matches the ACE to the inner VLAN ID of a double tagged packet.
- **802.1p** — Displays the packet tag value.
- **802.1p Mask** — Displays the wildcard bits to be applied to the CoS.
- **Ethertype** — Displays the Ethernet type of the packet.
- **Action** — Indicates the ACL forwarding action. The possible field values are:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.

#### **STEP 3** Define the relevant fields,

**STEP 4** Click **Apply**. The MAC Based ACL is modified, and the device is updated.

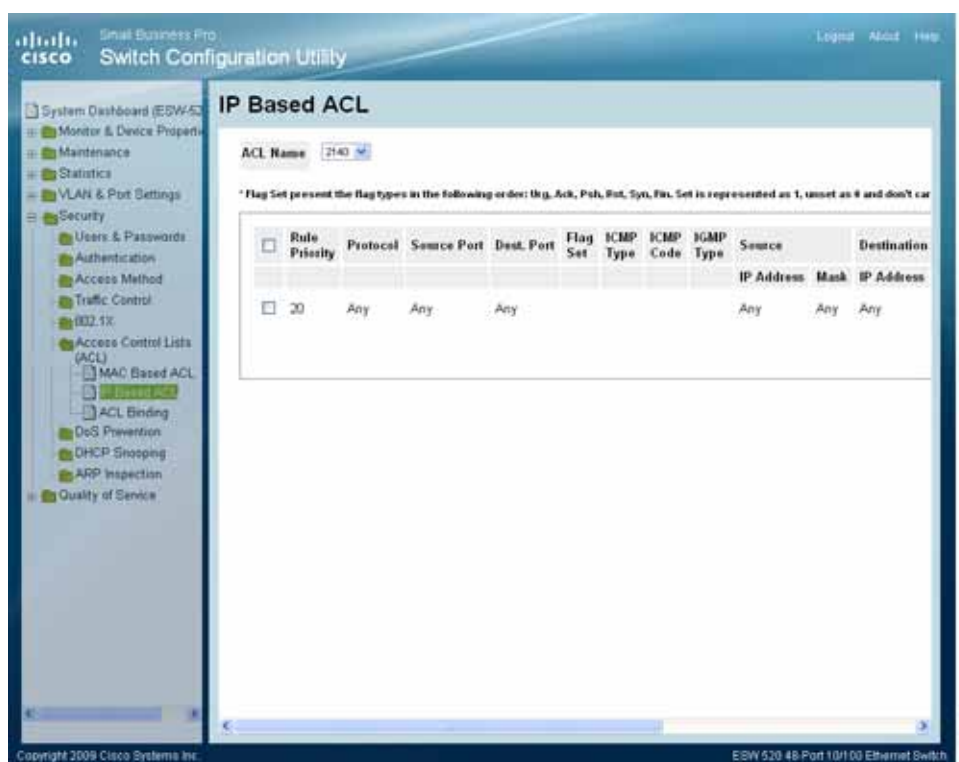
## Defining IP Based ACL

The *IP Based ACL Page* contains information for defining IP Based ACLs, including defining the ACEs defined for IP Based ACLs.

To define an IP based ACL:

**STEP 1** Click **Security** > **Access Control Lists (ACL)** > **IP Based ACL**. The *IP Based ACL Page* opens:

### IP Based ACL Page



The *IP Based ACL Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.



- **Protocol** — Creates an ACE based on a specific protocol. The possible field values are:
  - *ICMP* — *Internet Control Message Protocol* (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
  - *IGMP* — *Internet Group Management Protocol* (IGMP). Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.
  - *IP* — *Internet Protocol* (IP). Specifies the format of packets and their addressing method. IP addresses packets and forwards the packets to the correct port.
  - *TCP* — *Transmission Control Protocol* (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order they are sent.
  - *EGP* — *Exterior Gateway Protocol* (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
  - *IGP* — *Interior Gateway Protocol* (IGP). Allows for routing information exchange between gateways in an autonomous network.
  - *UDP* — *User Datagram Protocol* (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
  - *HMP* — *Host Mapping Protocol* (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
  - *RDP* — *Remote Desktop Protocol* (RDP). Allows a clients to communicate with the Terminal Server over the network.
  - *IDPR* — Matches the packet to the *Inter-Domain Policy Routing* (IDPR) protocol.
  - *RSVP* — Matches the packet to the *ReSerVation Protocol* (RSVP).
  - *GRE* — Matches the packet to the Generic Routing Encapsulation (GRE) protocol.
  - *ESP* — Matches the packet to the Encapsulating Security Payload (ESP) protocol.

- *AH* — *Authentication Header* (AH). Provides source host authentication and data integrity.
  - *EIGRP* — *Enhanced Interior Gateway Routing Protocol* (EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
  - *OSPF* — The *Open Shortest Path First* (OSPF) protocol is a link-state, hierarchical Interior Gateway Protocol (IGP) for network routing Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).
  - *IPIP* — *IP over IP* (IPIP). Encapsulates IP packets to create tunnels between two routers. This ensure that IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing.
  - *PIM* — Matches the packet to *Protocol Independent Multicast* (PIM).
  - *L2TP* — Matches the packet to *Layer 2 Internet Protocol* (L2IP).
  - *ISIS* — *Intermediate System - Intermediate System* (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks.
  - *ANY* — Matches the protocol to any protocol.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
  - **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
  - **Flag Set** — Sets the indicated TCP EtherChannel that can be triggered.
  - **ICMP Type** — Filters packets by ICMP message type. The field values is 0-255.
  - **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
  - **IGMP Type** — Filters packets by IGMP message or message types.
  - **Source**

- **IP Address** — Displays the source port IP address to which packets are addressed to the ACE.
- **Wildcard Mask** — Displays the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination**
  - **IP Address** — Displays the destination IP address to which packets are addressed to the ACE.
  - **Wildcard Mask** — Displays the destination IP address wildcard mask.
- **DCSP** — Matches the packets DSCP value.
- **IP Prec** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.
  - *Match IP Precedence* — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Delete ACL button** — To remove an ACL, click the **Delete ACL** button.
- **Delete Rule button** — To remove an ACE rule, click the **rule's checkbox** and click the **Delete Rule** button.

**STEP 2** Click the **Add ACL** button. The *Add IP Based ACL Page* opens:

#### Add IP Based ACL Page

**Add IP Based ACL**

ACL Name:

☐ New Rule Priority:

Protocol: ☒ ICMP ☐ Protocol ID To Match:

Source Port: ☐  ☒ Any

Destination Port: ☐  ☒ Any

TCP Flags: ☒ Urg:  Ack:  Psh:  Rst:  Syn:  Fin:

ICMP: ☐ Select from List:  ☐ ICMP Type:  ☒ Any

ICMP Code: ☐  ☒ Any

IGMP: ☒ Select from List:  ☐ IGMP Type:  ☒ Any

Source IP Address: ☒  WildCard mask:  ☐ Any

Destination IP Address: ☒  WildCard mask:  ☐ Any

Traffic Class: ☐ ☐ Match DSCP:  ☐ Match IP Precedence:

Action:

The *Add IP Based ACL Page* contains the following fields:

- **ACL Name** — Defines the user-defined IP based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IP Based ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP EtherChannel. Filtered packets are either forwarded or dropped. Filtering packets by TCP EtherChannels increases packet control, which increases network security. Once the box is checked, there are other parameters that can be selected from the dropdown menu:
  - Urg — Urgent
  - Ack — Acknowledgement

- Psh — Push
  - Rst — Reset
  - Syn — Synchronize
  - Fin — Final
- **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **ICMP Type** — Filters packets by IGMP message or message types
- **IGMP** — Filters packets by IGMP message or message types.
- **Source**
  - *IP Address* — Matches the source port IP address from which packets are addressed to the ACE.
  - *Wildcard Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination**
  - *IP Address* — Matches the destination port IP address to which packets are addressed to the ACE.
  - *Wildcard Mask* — Defines the destination IP address of the wildcard mask.

Select either **Match DSCP** or **Match IP Precedence**.

- **Match DSCP** — Matches the packet to the DSCP tag value. The possible field range is 0-63.
- **Match IP Precedence** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.

- **Traffic Class** — Indicates the traffic class to which the packets are matched. The possible field values are:
  - *Checked* — Matches packets to traffic classes.
  - *Unchecked* — Does not match packets to traffic classes.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

**STEP 3** Define the relevant fields,

**STEP 4** Click **Apply**. The IP Based ACL is defined, and the device is updated.

---

### Modifying IP Based ACL

---

**STEP 1** Click **Security > Access Control Lists (ACL) > IP Based ACL**. The *IP Based ACL Page* opens.

**STEP 2** Click the **Edit** button. The *Edit IP Based ACL Page* opens:

#### Edit IP Based ACL Page

**Edit IP Based ACL**

ACL Name:

New Rule Priority:

Protocol: ☒ ICMP ☐ Protocol ID To Match:  ☐ Any

Source Port: ☐  ☒ Any

Destination Port: ☐  ☒ Any

TCP Flags: ☐ Urg:  Ack:  Psh:  Rst:  Syn:  Fin:

ICMP: ☐ Select from List:  ☐ ICMP Type:  ☒ Any

ICMP Code: ☐  ☒ Any

IGMP: ☐ Select from List:  ☐ IGMP Type:  ☒ Any

Source IP Address: ☒  WildCard mask:  ☐ Any

Destination IP Address: ☒  WildCard mask:  ☐ Any

Traffic Class: ☐ ☐ Match DSCP:  ☐ Match IP Precedence:

Action:

The Edit IP Based ACL Page contains the following fields:

- **ACL Name** — Displays the user-defined based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *ACL Page* above.
- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP EtherChannel. Filtered packets are either forwarded or dropped. Filtering packets by TCP EtherChannels increases packet control, which increases network security.
- **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:

- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP** — Filters packets by IGMP message or message types.
- **Source**
  - *IP Address* — Matches the source port IP address from which packets are addressed to the ACE.
  - *Wildcard Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while the last eight bits are used.
- **Destination**
  - *IP Address* — Matches the destination port IP address to which packets are addressed to the ACE.
  - *Wildcard Mask* — Defines the destination IP address of the wildcard mask.
- Select either **Match DSCP** or **Match IP Precedence**.
  - **Match DSCP** — Matches the packet to the DSCP tag value.
  - **Match IP Precedence** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Traffic Class** — Indicates the traffic class to which the packet is matched.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shut down, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.



**STEP 3** Define the relevant fields,

**STEP 4** Click **Apply**. The IP Based ACL is modified, and the device is updated.

### Adding an IP Based Rule

**STEP 1** Click **Security > Access Control Lists (ACL) > IP Based ACL**. The *IP Based ACL Page* opens:

**STEP 2** Select an ACL from the ACL Name drop-down list.

**STEP 3** Click the **Add Rule** button. The *Add IP Based Rule Page* opens:

### Add IP Based Rule Page

The screenshot shows the 'Add IP Based Rule' configuration page. The fields are as follows:

- ACL Name:** acl2
- New Rule Priority:** 11
- Protocol:** ICMP (selected). Protocol ID To Match: Any (radio button).
- Source Port:** Any (radio button).
- Destination Port:** Any (radio button).
- TCP Flags:** Urg (Set), Ack (Set), Psh (Set), Rst (Set), Syn (Set), Fin (Set).
- ICMP:** Select from List: Echo Reply (selected). ICMP Type: Any (radio button).
- ICMP Code:** Any (radio button).
- IGMP:** Select from List: DVMRP (selected). IGMP Type: Any (radio button).
- Source IP Address:** WildCard mask: Any (radio button).
- Destination IP Address:** WildCard mask: Any (radio button).
- Traffic Class:** Match DSCP (radio button), Match IP Precedence (radio button).
- Action:** Permit (selected).

The 'Apply' button is located at the bottom right of the form.

The *Add IP Based Rule Page* contains the following fields:

- **ACL Name** — Displays the user-defined IP based ACLs.
- **New Rule Priority** — Indicates the rule priority, which determines which rule is matched to a packet on a first-match basis.
- **Protocol** — Creates an ACE based on a specific protocol. For a list of available protocols, see the **Protocol** field description in the *IP Based ACL Page* above.

- **Source Port** — Defines the TCP/UDP source port to which the ACE is matched. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
- **Destination Port** — Defines the TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down list. The possible field range is 0 - 65535.
- **TCP Flags** — Filters packets by TCP EtherChannel. Filtered packets are either forwarded or dropped. Filtering packets by TCP EtherChannels increases packet control, which increases network security.
- **ICMP** — Indicates if ICMP packets are permitted on the network. The possible field values are as follows:
- **ICMP Code** — Indicates and ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code.
- **IGMP** — Filters packets by IGMP message or message types.
- **Source IP Address** — Matches the source port IP address to which packets are addressed to the ACE.
- **Dest. IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.
- **Traffic Class** — Indicates the traffic class to which the packet is matched.
- Select either **Match DSCP** or **Match IP**:
  - **Match DSCP** — Matches the packet to the DSCP tag value.
  - **Match IP Precedence** — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-7.
- **Action** — Indicates the action assigned to the packet matching the ACL. Packets are forwarded or dropped. In addition, the port can be shutdown, a trap can be sent to the network administrator, or packet is assigned rate limiting restrictions for forwarding. The options are as follows:
  - *Permit* — Forwards packets which meet the ACL criteria.
  - *Deny* — Drops packets which meet the ACL criteria.
  - *Shutdown* — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the *Port Management* page.

**STEP 4** Define the relevant fields,

**STEP 5** Click **Apply**. The IP Based ACL is modified, and the device is updated.

## Defining ACL Binding

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface. Whenever an ACL is assigned on a port or a EtherChannel flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets. To bind ACLs to an interface:

**STEP 1** Click **Security > Access Control Lists (ACL) > ACL Binding**. The *ACL Binding Page* opens:

### ACL Binding Page



The *ACL Binding Page* contains the following fields:

- **Copy From Entry Number** — Copies the ACL binding configuration from the specified table entry.

- **To Entry Number(s)** — Assigns the copied ACL binding configuration to the specified table entry.
- **Ports/EtherChannels** — Indicates the interface to which the ACL is bound.

For each entry, an interface has a bound ACL.

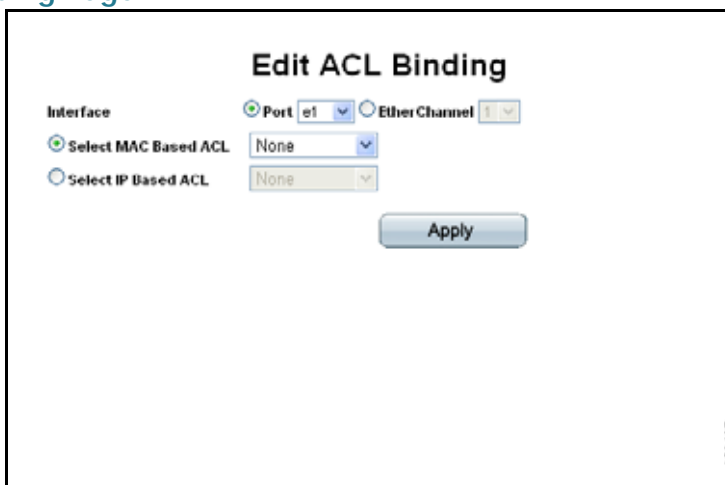
- **Interface** — Indicates the interface to which the associated ACL is bound.
- **ACL Name** — Indicates the ACL which is bound to the associated interface.
- **Type** — Indicates the ACL type to which is bound to the interface.

### Modifying ACL Binding

**STEP 1** Click **Security > Access Control Lists (ACL) > ACL Binding**. The *ACL Binding Page* opens:

**STEP 2** Click the **Edit** button. The *Edit ACL Binding Page* opens:

#### Edit ACL Binding Page



The *Edit ACL Binding Page* contains the following fields:

- **Interface** — Indicates the interface to which the ACL is bound.
- **Select MAC Based ACL** — Indicates the MAC based ACL which is bound to the interface.
- **Select IP Based ACL** — Indicates the IP based ACL which is bound to the interface.

**STEP 3** Define the relevant fields.

---

**STEP 4** Click **Apply**. The ACL binding is defined, and the device is updated.

---

## Defining DoS Prevention

*Denial of Service* (DOS) increases network security by preventing packets with invalid IP addresses from entering the network. DoS eliminates packets from malicious networks which can compromise a network's stability.

The device provides a Security Suite that allows administrators to match, discard, and redirect packets based on packet header values. Packets which are redirected are analyzed for viruses and Trojans.

DoS enables network managers to:

- Deny packets that contain reserved IP addresses
- Prevent TCP connections from a specific interface
- Discard echo requests from a specific interface
- Discard IP fragmented packets from a specific interface

The DoS Prevention section contains the following pages:

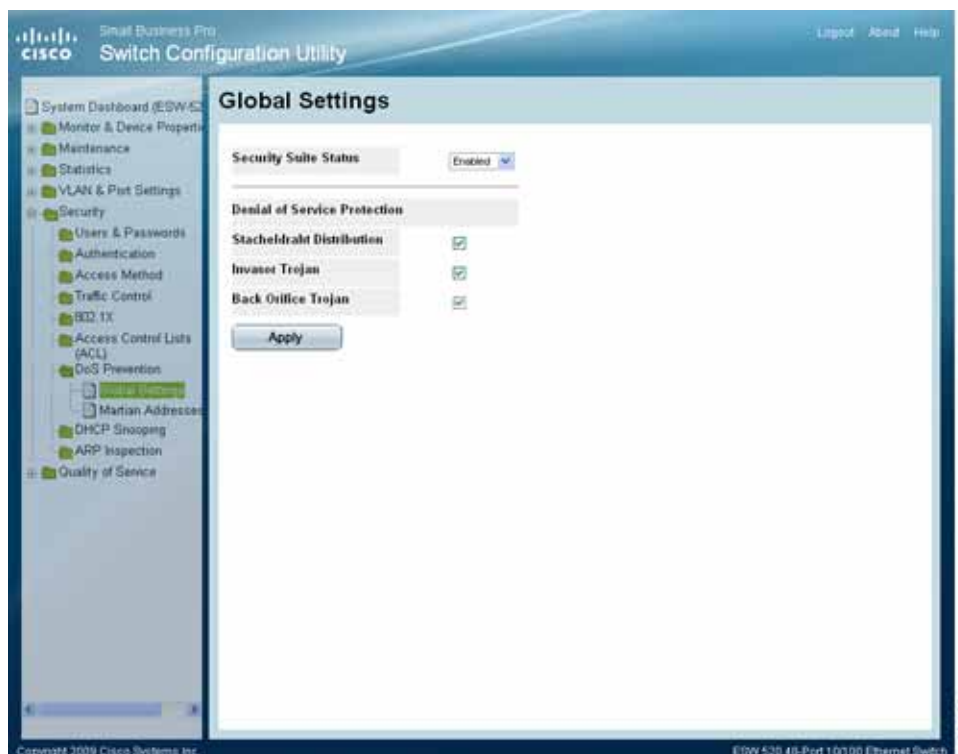
- DoS Global Settings
- Defining Martian Addresses

### DoS Global Settings

The *Global Settings Page* allows network managers to enable and define global DoS attack prevention parameters on the device. To open the *Global Settings Page*:

- STEP 1** Click **Security > DoS Prevention > Global Settings**. The *Global Settings Page* opens:

#### Global Settings Page



The *Global Settings Page* contains the following fields:

- **Security Suite Status** — Indicates if DoS security is enabled on the device. The possible field values are:
  - *Enable* — Enables DoS security.
  - *Disable* — Disables DoS security on the device. This is the default value.
- **Denial of Service Protection** — Indicates if any of the services listed below are enabled. If the service protection is disabled, the *Stacheldraht Distribution*, *Invasor Trojan*, and *Back Office Trojan* fields are disabled.
- **Stacheldraht Distribution** — Discards TCP packets with source TCP port equal to 16660
- **Invasor Trojan** — Discards TCP packets with destination TCP port equal to 2140 and source TCP port equal to 1024.

- **Back Orifice Trojan** — Discards UDP packets with destination UDP port equal to 31337 and source UDP port equal to 1024.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The DoS prevention global settings are defined, and the device is updated.

---

## Defining Martian Addresses

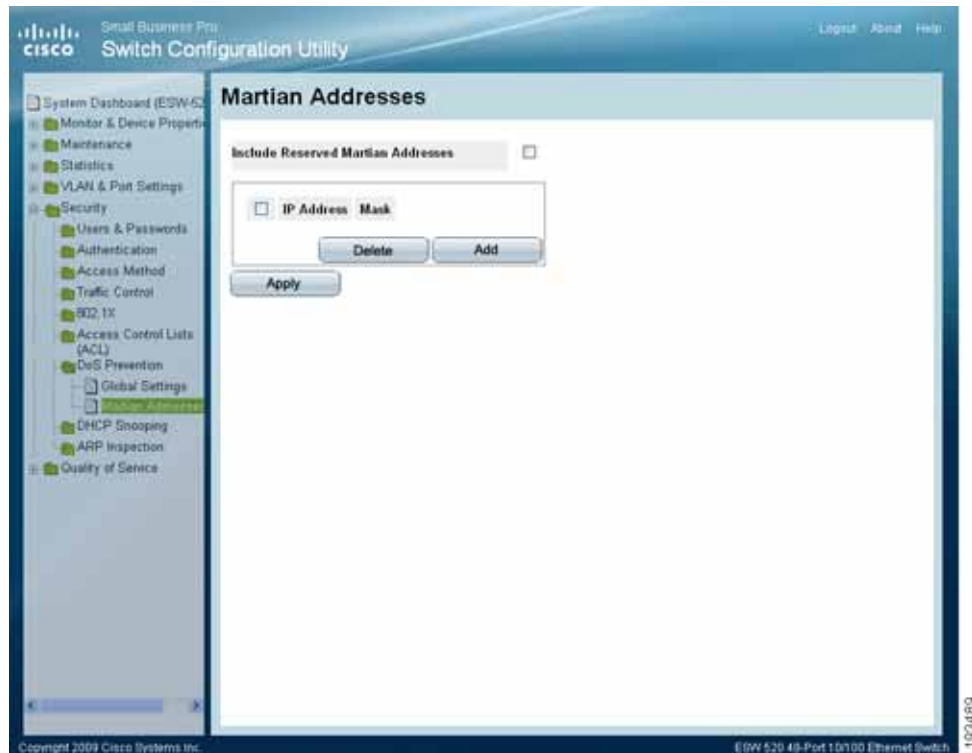
Martian Address Filtering enables discarding IP packets from invalid IP addresses. Martian addresses include packets from a source IP addresses outside or not used within the configured network. Martian addresses include any address within the following ranges:

- **0.0.0.0/8 (Except 0.0.0.0/32 as a Source Address)** — Addresses in this block refer to source hosts on this network.
- **127.0.0.0/8** — Used as the Internet host loopback address.
- **192.0.2.0/24** — Used as the TEST-NET in documentation and example codes.
- **224.0.0.0/4 (As a Source IP Address)** — Used in Multicast address assignments, and This formerly known as Class D Address Space.
- **240.0.0.0/4 (Except 255.255.255.255/32 as a Destination Address)** — Reserved address range, and is formerly known as Class E Address Space.

To define Martian Addresses:

- STEP 1** Click **Security > DoS Prevention > Martian Addresses**. The *Martian Addresses Page* opens:

#### Martian Addresses Page



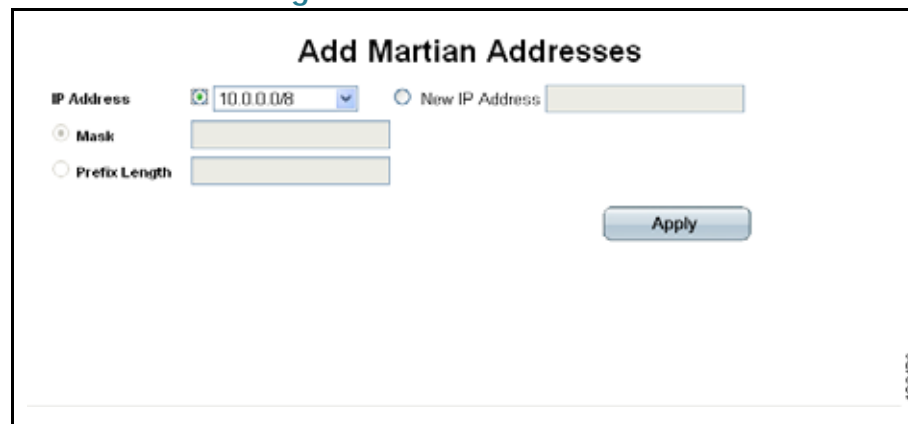
The *Martian Addresses Page* contains the following fields:

- **Include Reserved Martian Addresses** — Indicates that packets arriving from Martian addresses are dropped. Enabled is the default value. When enabled, the following IP addresses are included:
  - 0.0.0.0/8 (except 0.0.0.0/32), 127.0.0.0/8
  - 192.0.2.0/24 , 224.0.0.0/4
  - 240.0.0.0/4 (except 255.255.255.255/32)
- **IP Address** — Displays the IP addresses for which DoS attack is enabled.
- **Mask** — Displays the Mask for which DoS attack is enabled.
- **Delete** — To remove a Martian address, click the entry's checkbox and click the delete button.

- STEP 2** Click the **Add** button. The *Add Martian Addresses Page* opens:



#### Add Martian Addresses Page



The Add Martian Addresses Page contains the following fields:

- **IP Address** — Enter the Martian IP addresses for which DoS attack is enabled. The possible values are:
  - One of the addresses in the Martian IP address list.
  - New IP Address — Enter an IP Address that is not on the list.
- **Mask** — Enter the Mask for which DoS attack is enabled.
- **Prefix Length** — Defines the IP route prefix for the destination IP.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The martian addresses are added, and the device is updated.

## Defining DHCP Snooping

DHCP Snooping enables network administrators to differentiate between trusted interfaces connected to the DHCP servers and untrusted interfaces connected to a DHCP client.

DHCP Snooping filters untrusted messages. DHCP Snooping creates and maintains a DHCP Snooping Table which contains information received from untrusted packets. Interfaces are untrusted if the packet is received from an interface from outside the network or from a interface beyond the network firewall. Trusted interfaces receive packets only from within the network or the network firewall.

The *DHCP Snooping Table* contains the untrusted interfaces MAC address, IP address, Lease Time, VLAN ID, and interface information.

The DHCP Snooping section contains the following topics:

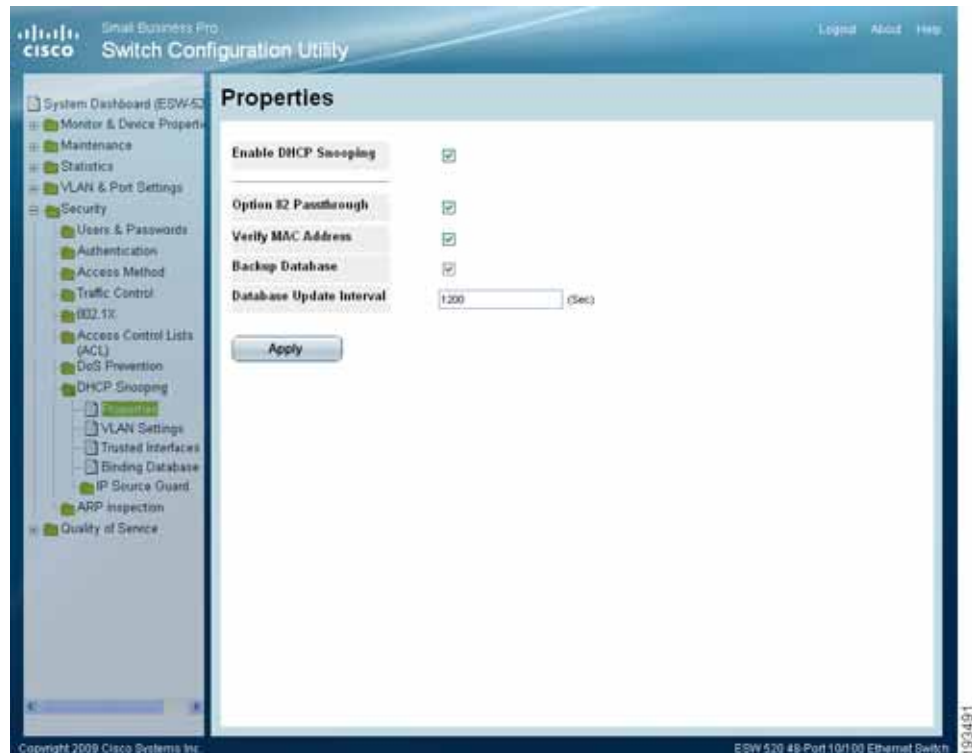
- Defining DHCP Snooping Properties
- Defining DHCP Snooping on VLANs
- Defining Trusted Interfaces
- Binding Addresses to the DHCP Snooping Database
- Defining IP Source Guard

### Defining DHCP Snooping Properties

The *DHCP Snooping Properties Page* contains parameters for enabling DHCP Snooping on the device. To define the DHCP Snooping general properties:

- STEP 1** Click **Security > DHCP Snooping > Properties**. The *DHCP Snooping Properties Page* opens:

#### DHCP Snooping Properties Page



The *DHCP Snooping Properties Page* contains the following fields:

- **Enable DHCP Snooping** — Indicates if DHCP Snooping is enabled on the device. The possible field values are:
  - *Checked* — Enables DHCP Snooping on the device.
  - *Unchecked* — Disables DHCP Snooping on the device. This is the default value.
- **Option 82 Passthrough** — Indicates if the device forwards or rejects packets that include Option 82 information, while DHCP Snooping is enabled.
  - *Checked* — Device forwards packets containing Option 82 information.
  - *Unchecked* — Device rejects packets containing Option 82 information.
- **Verify MAC Address** — Indicates if the MAC address is verified. The possible field values are:

- *Checked* — Verifies (on an untrusted port) that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header (part of the payload).
  - *Unchecked* — Disables verifying that the source MAC address of the Layer 2 header matches the client hardware address as appears in the DHCP Header. This is the default value.
- **Backup Database** — Indicates if the DHCP Snooping Database learning and update is enabled. All changes to the binding storage file are implemented only if the device's system clock is synchronized with the SNTP Server. The possible field values are:
  - *Checked* — Enables backing up of the allotted IP address in the DHCP Snooping Database.
  - *Unchecked* — Disables backing up to the allotted IP address in the DHCP Snooping Database. This is the default value.
- **Database Update Interval** — Indicates how often the DHCP Snooping Database is backed up. The possible field range is 600 – 86400 seconds. The field default is 1200 seconds.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The DHCP Snooping configuration is defined and the device is updated.

---

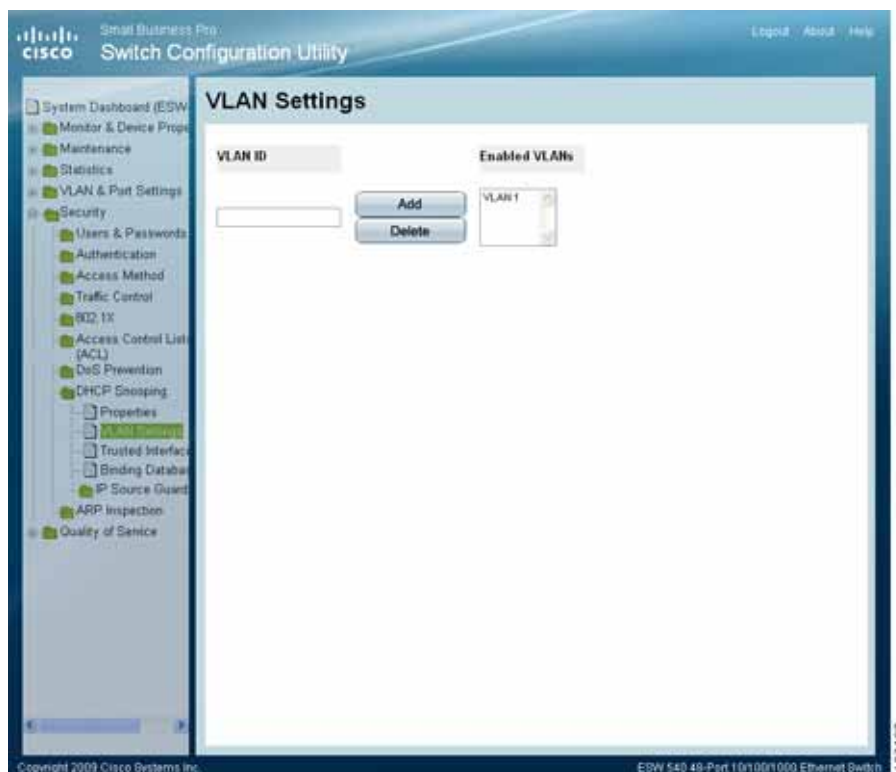
## Defining DHCP Snooping on VLANs

The *DHCP Snooping VLAN Settings Page* allows network managers to enable DHCP snooping on VLANs. To enable DHCP Snooping on a VLAN, ensure DHCP Snooping is enabled on the device.

To define DHCP Snooping on VLANs:

- STEP 1** Click **Security > DHCP Snooping > VLAN Settings**. The *DHCP Snooping VLAN Settings Page* opens:

#### DHCP Snooping VLAN Settings Page



The *DHCP Snooping VLAN Settings Page* contains the following fields:

- **VLAN ID** — Indicates the VLAN to be added to the Enabled VLAN list.
- **Enabled VLANs** — Contains a list of VLANs for which DHCP Snooping is enabled.

- STEP 2** Enter the VLAN name from the VLAN ID list and click **Add**. This VLAN name then appears in the **Enabled VLANs** list.

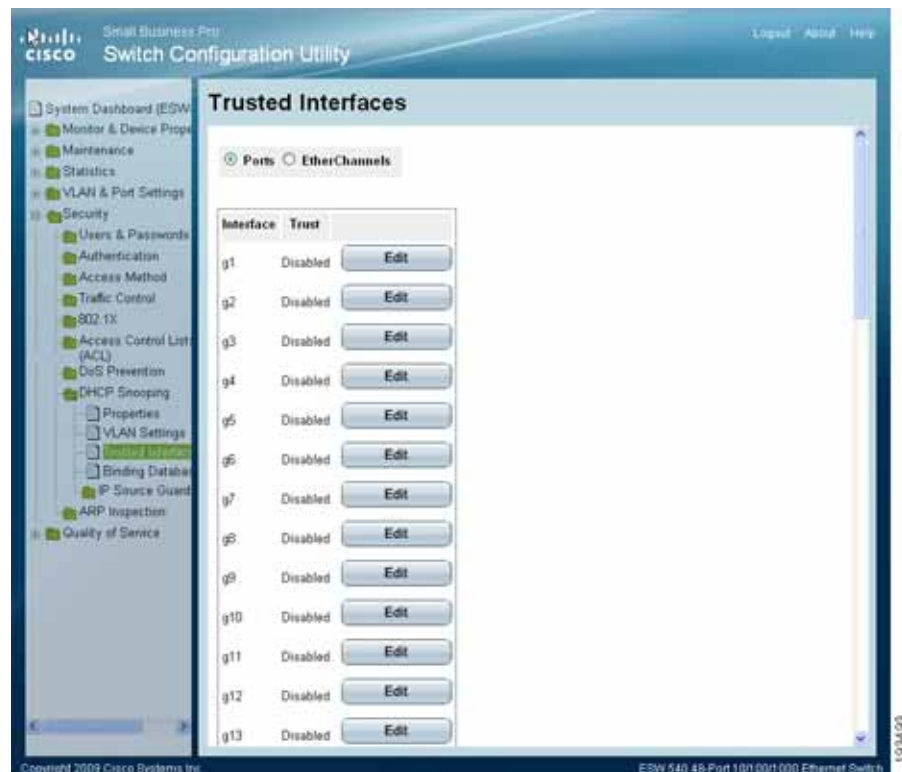
## Defining Trusted Interfaces

The *Trusted Interfaces Page* allows network managers to define Trusted interfaces. The device transfers all DHCP requests to trusted interfaces.

To define trusted interfaces:

- STEP 1** Click **Security > DHCP Snooping > Trusted Interfaces**. The *Trusted Interfaces Page* opens:

#### Trusted Interfaces Page



The *Trusted Interfaces Page* contains the following fields:

- **Ports** — Displays the ports which can be defined as trusted.
- **EtherChannels** — Displays the EtherChannels which can be defined as trusted.

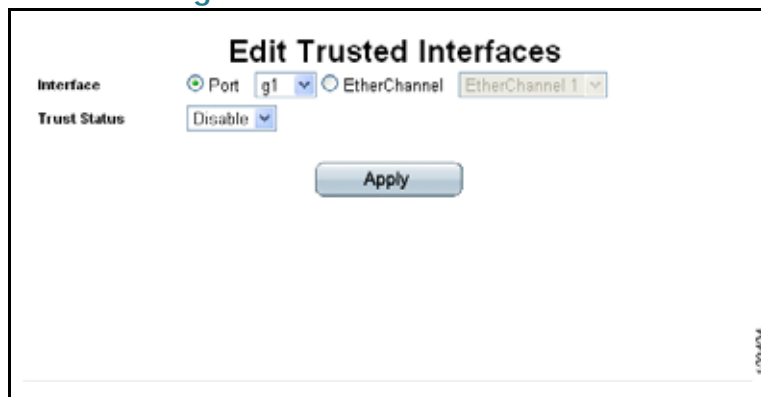
#### Trusted Interface Table

- **Interface** — Contains a list of existing interfaces.
- **Trust** — Indicates whether the interface is a Trusted interface.

- STEP 2** From the global **Interface** field, select either Ports or EtherChannels radio button.

- STEP 3** In the table, select an interface and click **Edit**. The *Edit Trusted Interface Page* opens.

#### Edit Trusted Interface Page

The screenshot shows a web-based configuration interface titled "Edit Trusted Interfaces". It contains two main sections: "Interface" and "Trust Status". In the "Interface" section, there are two radio buttons: "Port" (which is selected) and "EtherChannel". Next to "Port" is a dropdown menu showing "g1". Next to "EtherChannel" is a dropdown menu showing "EtherChannel 1". In the "Trust Status" section, there is a dropdown menu showing "Disable". Below these sections is a large "Apply" button. The interface is enclosed in a rectangular frame with a small vertical label "1/20/2014" on the right side.

The *Edit Trusted Interface Page* contains the following field:

- **Interface** — Contains a list of existing interfaces.
- **Trust Status** — Indicates whether the interface is a Trusted Interface.
  - *Enable* — Interface is in trusted mode.
  - *Disable* — Interface is in untrusted mode.

**STEP 4** Define the fields.

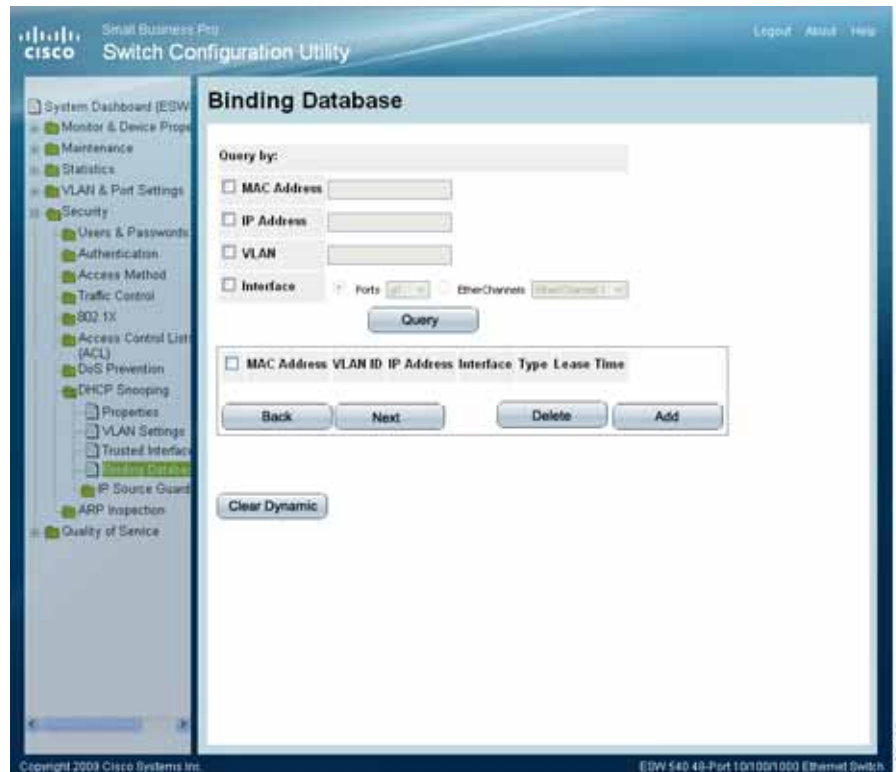
**STEP 5** Click **Apply**. The Trusted Interfaces configuration is defined and the device is updated.

#### Binding Addresses to the DHCP Snooping Database

The *Binding Database Page* contains parameters for querying and adding IP addresses to the DHCP Snooping Database. To bind addresses to the DHCP Snooping database:

- STEP 1** Click **Security > DHCP Snooping > Binding Database**. The *Binding Database Page* opens:

#### Binding Database Page



- STEP 2** Define any of the following fields as a query filter:

#### Query By

- **MAC Address** — Indicates the MAC addresses recorded in the DHCP Database. The Database can be queried by MAC address.
- **IP Address** — Indicates the IP addresses recorded in the DHCP Database. The Database can be queried by IP address.
- **VLAN** — Indicates the VLANs recorded in the DHCP Database. The Database can be queried by VLAN.
- **Interface** — Contains a list of interface by which the DHCP Database can be queried. The possible field values are:
  - *Ports* — Queries the VLAN database by a port number.



- *EtherChannel* — Queries the VLAN database by EtherChannel number.

**STEP 3** Click **Query**. The results appear in the Query Results table.

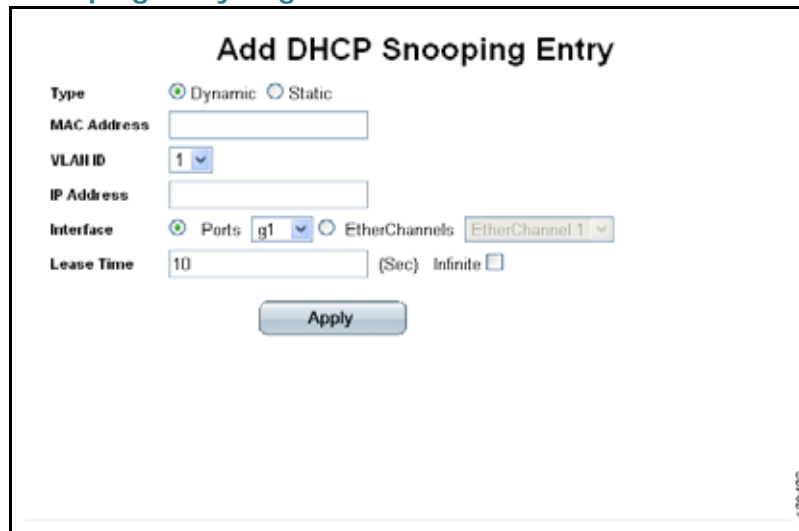
### Query Results

The Query Results table contains the following fields:

- **MAC Address** — Indicates the MAC address found during the query.
- **VLAN ID** — Displays the VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- **IP Address** — Indicates the IP address found during the query.
- **Interface** — Indicates the specific interface connected to the address found during the query.
- **Type** — Displays the IP address binding type. The possible field values are:
  - *Static* — Indicates the IP address is static.
  - *Dynamic* — Indicates the IP address is defined as a dynamic address in the DHCP database.
  - *Learned* — Indicates the IP address is dynamically defined by the DHCP server. (This field appears as a read-only field in the table).
- **Lease Time** — Displays the lease time. The Lease Time defines the amount of time the DHCP Snooping entry is active. Addresses whose lease times are expired are deleted from the database. The possible values are 10 – 4294967295 seconds. In the *Add DHCP Snooping Entry Page*, select **Infinite** if the DHCP Snooping entry never expires.

**STEP 4** Click **Add**. The *Add DHCP Snooping Entry Page* opens.

#### Add DHCP Snooping Entry Page



The screenshot shows a web-based configuration window titled "Add DHCP Snooping Entry". It contains several input fields and radio buttons. The "Type" field has two radio buttons: "Dynamic" (selected) and "Static". The "MAC Address" field is an empty text box. The "VLAN ID" field is a dropdown menu showing "1". The "IP Address" field is an empty text box. The "Interface" field has two radio buttons: "Ports" (selected) and "EtherChannels". The "Ports" radio button has a dropdown menu showing "g1". The "EtherChannels" radio button has a dropdown menu showing "EtherChannel 1". The "Lease Time" field is a text box showing "10" followed by "(Sec)" and an "Infinite" checkbox. An "Apply" button is at the bottom center. A small version number "1.024.025" is visible in the bottom right corner of the window.

The window displays the following fields:

- **Type** — Displays the IP address binding type. The possible field values are:
  - *Static* — Indicates the IP address is static.
  - *Dynamic* — Indicates the IP address is defined as a dynamic address in the DHCP database.
- **VLAN ID** — Displays the VLAN ID to which the IP address is attached in the DHCP Snooping Database.
- **IP Address** — Indicates the IP address found during the query.
- **Interface** — Indicates the specific interface connected to the address found during the query.

**Lease Time** — Displays the lease time.

**STEP 5** Define the fields.

**STEP 6** Click **Apply**. The bound address is added to the DHCP Snooping database and the device is updated.

**STEP 7** Click **Delete** to delete the data from the Query Results Table.

**STEP 8** To remove dynamic addresses from the Query Results table, click **Clear Dynamic**.

## Defining IP Source Guard

IP Source Guard is a security feature that restricts the client IP traffic to those source IP addresses configured in the DHCP Snooping Binding Database and in manually configured IP source bindings. For example, IP Source Guard can help prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

- DHCP snooping must be enabled on the device's untrusted interfaces and on the relevant VLAN, in order to activate the IP source guard feature.
- IP Source Guard must be enabled globally in the *IP Source Guard Properties Page* before it can be enabled on the device interfaces.
- IP Source Guard uses Ternary Content Addressable Memory (TCAM) resources, requiring use of 1 TCAM rule per 1 IP Source Guard address entry. If the number of IP Source Guard entries exceeds the number of available TCAM rules, new IP source guard addresses remain inactive.
- IP Source Guard cannot be configured on routed ports.
- If IP Source Guard and MAC address filtering is enabled on a port, Port Security cannot be activated on the same port.
- If a port is trusted, filtering of static IP addresses can be configured, although IP Source Guard is not active in that condition.
- If a port's status changes from untrusted to trusted, the static IP address filtering entries remain but become inactive.

The IP Source Guard section contains the following topics:

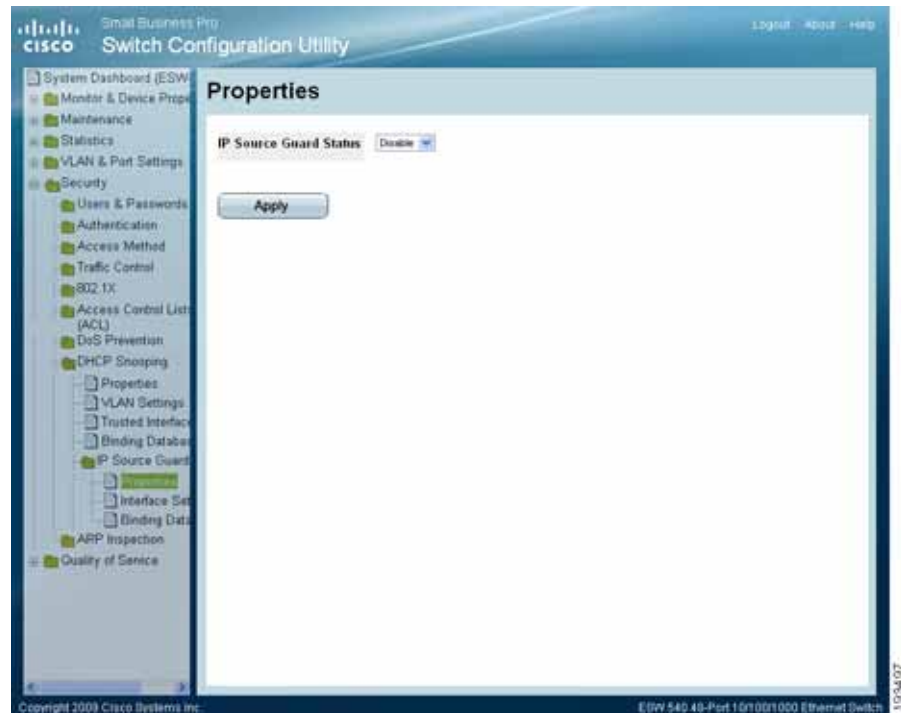
- Configuring IP Source Guard Properties
- Defining IP Source Guard Interface Settings
- Querying the IP Source Binding Database

## Configuring IP Source Guard Properties

The *IP Source Guard Properties Page* allows network managers to enable the use of IP Source Guard on the device. IP Source Guard must be enabled for the device before it can be enabled on individual ports or EtherChannels. To enable IP Source Guard:

- STEP 1** Click **Security > DHCP Snooping > IP Source Guard > Properties**. The *IP Source Guard Properties Page* opens:

#### IP Source Guard Properties Page



The *IP Source Guard Properties Page* contains the following fields:

- **IP Source Guard Status** — Enables the use of IP Source Guard status on the device.
  - *Enable* — Indicates that IP Source Guard is enabled for the device.
  - *Disable* — Indicates that IP Source Guard is disabled for the device.

- STEP 2** Enable or Disable use of IP Source Guard on the device.

- STEP 3** Click **Apply**. The IP Source Guard configuration is modified, and the device is updated.

#### Defining IP Source Guard Interface Settings

In the *IP Source Guard Interface Settings Page*, IP Source Guard can be enabled on DHCP Snooping untrusted interfaces, permitting the transmission of DHCP packets allowed by DHCP Snooping. If source IP address filtering is enabled, packet transmission is permitted as follows:

- **IPv4 traffic** — Only IPv4 traffic with a source IP address that is associated with the specific port is permitted.
- **Non IPv4 traffic** — All non-IPv4 traffic is permitted.

**NOTE:** IP Source Guard must be enabled globally in the *IP Source Guard Properties Page* before it can be enabled on the device interfaces.

If a port is trusted, filtering of static IP addresses can be configured, although IP Source Guard is not active in that condition.

If a port's status changes from untrusted to trusted, the static IP address filtering entries remain but become inactive.

- STEP 1** Click **Security > DHCP Snooping > IP Source Guard > Interface Settings**. The *IP Source Guard Interface Settings Page* opens:

#### IP Source Guard Interface Settings Page



The *IP Source Guard Interface Settings Page* contains the following radio buttons and fields:

- **Ports** — Displays the port on which the IP source guard is enabled.
- **EtherChannels** — Displays the EtherChannels on which the IP source guard is enabled.
- **Interface** — Indicates the port's or EtherChannel's number.
- **Status** — Indicates if IP Source Guard is enabled or disabled.
  - *Enable* — Indicates that IP Source Guard is enabled on the interface.
  - *Disable* — Indicates that IP Source Guard is disabled on the interface. This is the default value.

- STEP 2** Click **Edit**. The *Edit Interface Settings Page* opens:

#### Edit Interface Settings Page



**Edit Interface Settings**

Interface ☒ Port g1 ☐ Ether Channel 1

Status Disable

**Apply**

**STEP 3** Define the fields.

**STEP 4** Click **Apply**. The new IP Source Guard Interface configuration is added, and the device is updated.

#### Querying the IP Source Binding Database

The *IP Source Guard Binding Database Page* enables network managers to query and view information about inactive addresses recorded in the DHCP Database. To query the IP Source Guard Database:

**STEP 1** Click **Security > DHCP Snooping > IP Source Guard > Binding Database**. The *IP Source Guard Binding Database Page* opens:

#### IP Source Guard Binding Database Page

The screenshot shows the Cisco Switch Configuration Utility interface for an ESW 520-48 switch. The left sidebar contains a tree view with the following structure: System Dashboard (ESW 520-48), Monitor & Device Properties, Maintenance, Statistics, VLAN & Port Settings, Security (expanded), Users & Passwords, Authentication, Access Method, Traffic Control, 802.1X, Access Control Lists (ACL), DoS Prevention, DHCP Snooping (expanded), Properties, VLAN Settings, Trusted Interfaces, Binding Database (selected), IP Source Guard, Properties, Interface Settings, Binding Database, ARP Inspection, and Quality of Service. The main content area is titled "Binding Database". It includes a "TCAM Resources" section with a "Retry Frequency" field set to 60 (Sec) and an "Insert Inactive" section with radio buttons for "Never" and "Retry Now". Below this is a "Query by:" section with checkboxes for "MAC Address", "IP Address", "VLAN", and "Interface". The "Interface" checkbox is selected, and it has sub-selects for "Ports" and "EtherChannels". A "Query" button is located below these options. At the bottom, there is a table with columns: Interface, Status, IP Address, VLAN, MAC Address, Type, and Reason. Below the table are "Back", "Next", and "Apply" buttons. The footer of the page includes "Copyright 2008 Cisco Systems Inc." and "ESW 520 48-Port 10/100 Ethernet Switch with PoE".

The *IP Source Guard Binding Database Page* contains the following fields:

#### TCAM Resources

- **Insert Inactive** — The IP Source Guard Database uses the TCAM resources for managing the database. If TCAM resources are not available, IP source guard addresses may become inactive. The switch can try to activate inactive addresses in various time intervals:
  - *Retry Frequency* — Try to activate inactive addresses at a specified interval. The possible values are 10 - 600 seconds.
  - *Never* — Never try to activate inactive addresses.
  - *Retry Now* — Try to activate inactive addresses immediately



#### Query By

**STEP 2** In the Query By section, select and define the preferred filter for searching the IP Source Guard Database:

- **MAC Address** — Queries the database by MAC address.
- **IP Address** — Queries the database by IP address.
- **VLAN** — Queries the database by VLAN ID.
- **Interface** — Queries the database by interface number. The possible field values are:
  - *Port* — Queries the database by a specific port number.
  - *EtherChannel* — Queries the VLAN database by EtherChannel number.

**STEP 3** Click **Query**. The results appear in the Query Results table.

#### Query Results

The Query Results table contains the following fields:

- **Interface** — Displays the interface number.
- **Status** — Displays the current interface status. The possible field values are:
  - *Active* — Indicates the interface is currently active.
  - *Inactive* — Indicates the interface is currently inactive.
- **IP Address** — Indicates IP address of the interface.
- **VLAN** — Indicates if the address is associated with a VLAN.
- **MAC Address** — Displays the MAC address of the interface.
- **Type** — Displays the IP address type. The possible field values are:
  - *Dynamic* — Indicates the IP address is dynamically created.
  - *Static* — Indicates the IP address is a static IP address.
  - *Learned* — Indicates the IP address is dynamically defined by the DHCP server. (This field appears as a read-only field in the table).
- **Reason** — Displays the reason an IP source address is inactive. The possible field options are:
  - *No Problem* — Indicates the IP address is active.

- *VLAN* — Indicates that DHCP Snooping is not enabled on the VLAN.
- *Trusted Port* — Indicates the port is a trusted port.
- *Resource Problem* — Indicates that the TCAM is full.

**STEP 4** Define the relevant fields. Click **Apply** and the device is updated.

## Defining Dynamic ARP Inspection

*Dynamic Address Resolution Protocol* (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses. Classic ARP does the following:

- Permits two hosts on the same network to communicate and send packets.
- Permits two hosts on different networks to communicate via a gateway.
- Permits routers to send packets via a host to a different router on the same network.
- Permits routers to send packets to a destination host via a local host.

ARP Inspection intercepts, discards, and logs ARP packets that contain invalid IP-to-MAC address bindings. This eliminates man-in-the-middle attacks, where false ARP packets are inserted into the subnet. Packets are classified as:

- **Trusted** — Indicates that the interface IP and MAC address are recognized, and recorded in the ARP Inspection List. Trusted packets are forwarded without ARP Inspection.
- **Untrusted** — Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
  - *Source MAC* — Compares the packet's source MAC address in the Ethernet header against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.
  - *Destination MAC* — Compares the packet's destination MAC address in the Ethernet header against the destination interface's MAC address. This check is performed for ARP responses.
  - *IP Addresses* — Checks the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses.

If the packet's IP address was not found in the ARP Inspection List, and DHCP snooping is enabled for a VLAN, a search of the DHCP Snooping Database is performed. If the IP address is found, the packet is valid and is forwarded.



**NOTE** ARP inspection is performed only on untrusted interfaces.

The ARP Inspection section contains the following topics:

- Defining ARP Inspection Properties
- Defining ARP Inspection Trusted Interfaces
- Defining ARP Inspection List
- Assigning ARP Inspection VLAN Settings

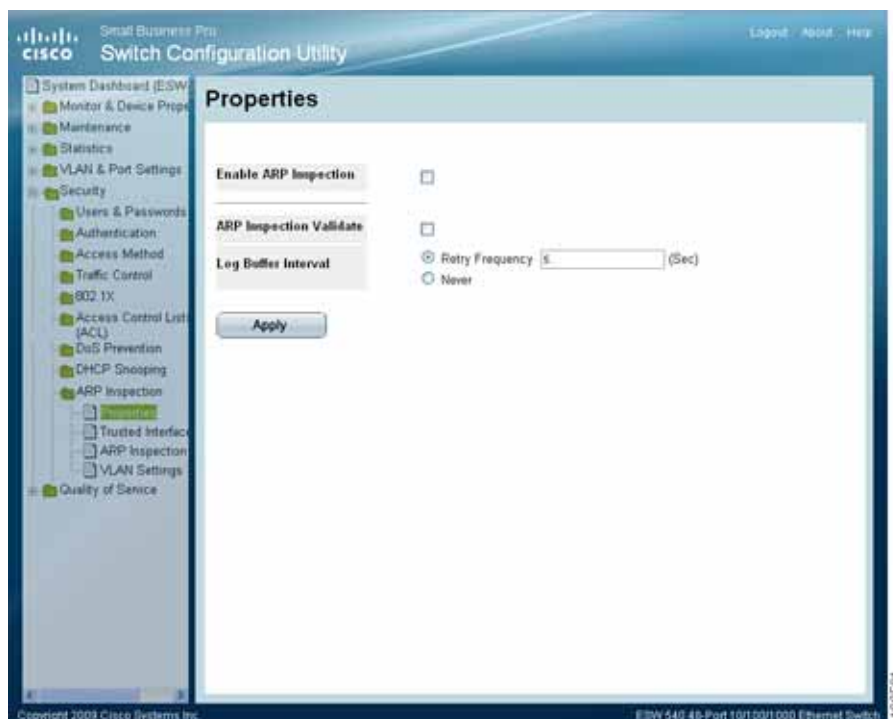
### Defining ARP Inspection Properties

The *ARP Inspection Properties Page* provides parameters for enabling and setting global Dynamic ARP Inspection parameters, as well as defining ARP Inspection Log parameters.

To define ARP Inspection properties:

- STEP 1** Click **Security > ARP Inspection > Properties**. The *ARP Inspection Properties Page* opens:

#### ARP Inspection Properties Page



The *ARP Inspection Properties Page* contains the following fields:

- **Enable ARP Inspection** — Enables ARP Inspection on the device. The possible field values are:
  - *Checked* — Enables ARP Inspection on the device.
  - *Unchecked* — Disables ARP Inspection on the device. This is the default value.
- **ARP Inspection Validate** — Enables ARP Inspection Validation on the device. The possible field values are:
  - *Checked* — Enables ARP Inspection Validation on the device. Source MAC, Destination MAC, and IP addresses are checked in ARP requests and responses.
  - *Unchecked* — Disable ARP Inspection Validation on the device. This is the default value.

- **Log Buffer Interval** — Defines the minimal interval between successive Syslog messages. The possible field values are:
  - *Retry Frequency* — Frequency at which the log is updated. The possible range is 0-86400 seconds. 0 seconds specifies immediate transmissions of Syslog messages. The default value is 5 seconds.
  - *Never* — Log is never updated.

**STEP 2** Define the fields.

**STEP 3** Click **Apply**. The ARP Inspection settings are modified, and the device is updated.

---

## Defining ARP Inspection Trusted Interfaces

The *ARP Inspection Trusted Interfaces Page* allows network managers to define trusted and untrusted interfaces. These settings are independent of the trusted interface settings defined for DHCP snooping. ARP Inspection is enabled only on untrusted interfaces.

To define trusted interfaces:

- STEP 1** Click **Security > ARP Inspection > Trusted Interfaces**. The *ARP Inspection Trusted Interfaces Page* opens:

#### ARP Inspection Trusted Interfaces Page



The *ARP Inspection Trusted Interfaces Page* contains the following fields:

- **Ports** — Specifies the Port on which ARP Inspection Trust mode can be enabled.
- **EtherChannels** — Specifies the EtherChannel for which the Trusted Interface settings are displayed.
- **Interface** — Displays the interface on which edits can be made.
- **Trust** — Enables or disables ARP Inspection Trust mode on the interface. The possible field values are:
  - *Enable* — Indicates the port or EtherChannel is a trusted interface, and ARP inspection is not performed on the ARP requests/replies sent to/from the interface.
  - *Disable* — Indicates the port or EtherChannel is not a trusted interface, and ARP inspection is performed on the ARP requests/replies sent to/from the interface. This is the default value.

**STEP 2** Click **Edit**. The *Edit Interface Settings Page* opens:

#### Edit Interface Settings Page



**STEP 3** Define the fields.

**STEP 4** Click **Apply**. The Trusted Interface's configuration is modified, and the device is updated.

## Defining ARP Inspection List

The *ARP Inspection List Page* provides information for creating static ARP Binding Lists. ARP Binding Lists contain the List Name, IP address and MAC address which are validated against ARP requests and replies.

To add an ARP Inspection List entry:

- STEP 1** Click **Security > ARP Inspection > ARP Inspection List**. The *ARP Inspection List Page* opens:

#### ARP Inspection List Page



The *ARP Inspection List Page* contains the following fields:

- **ARP Inspection List Name** — Pull-down lists name of the Inspection List.
- **Delete and Add Buttons** — Delete or Add user-defined ARP Inspection Lists.

#### Static ARP Inspection Table

- **IP Address** — Specifies IP address included in ARP Binding Lists which is checked against ARP requests and replies.
- **MAC Address** — Specifies MAC address included in ARP Binding Lists which is checked against ARP requests and replies.

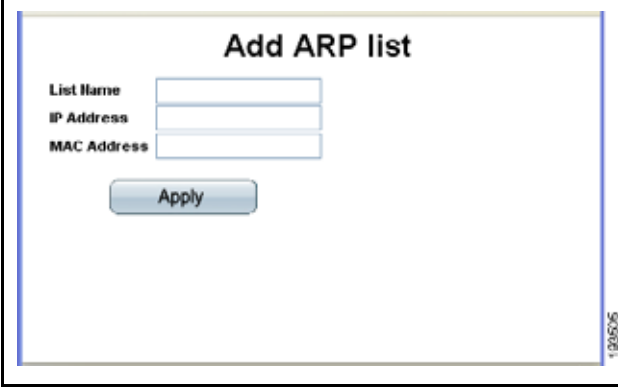


**NOTE** The Binding list cannot be added until an ARP list is added.

- STEP 2** Click **Add** under ARP Inspection List Name. The *Add ARP list Page* opens:



#### Add ARP list Page

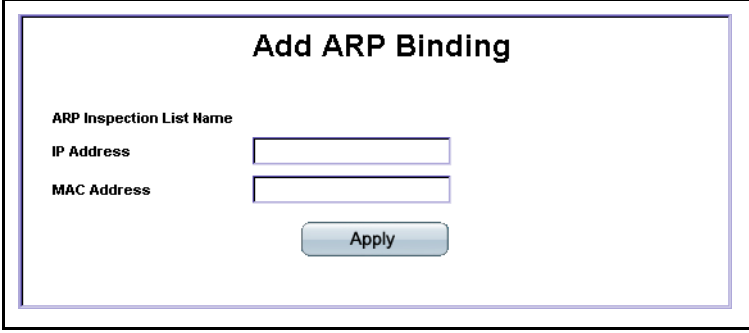
A screenshot of a web-based configuration page titled "Add ARP list". The page contains three input fields: "List Name", "IP Address", and "MAC Address", each with a corresponding text label to its left. Below these fields is a blue "Apply" button. The entire form is enclosed in a thin blue border.

- STEP 3** Define the fields and click **Apply**. The new ARP Inspection List is added and the device is updated.

#### Adding a Binding List entry

- STEP 1** Select an ARP Inspection List Name from the drop-down list.
- STEP 2** Click **Add** under Static ARP Table. The *Add ARP Binding Page* opens:

#### Add ARP Binding Page

A screenshot of a web-based configuration page titled "Add ARP Binding". The page contains three input fields: "ARP Inspection List Name", "IP Address", and "MAC Address", each with a corresponding text label to its left. Below these fields is a blue "Apply" button. The entire form is enclosed in a thin blue border.

- STEP 3** Define the fields.
- STEP 4** Click **Apply**. The add ARP Binding entry is added, and the device is updated.

## Assigning ARP Inspection VLAN Settings

The *ARP Inspection VLAN Settings Page* contains fields for enabling ARP Inspection on VLANs. In the Enabled VLAN table, users assign static ARP Inspection Lists to enabled VLANs. When a packet passes through an untrusted interface which is enabled for ARP Inspection, the device performs the following checks in order:

- Determines if the packet's IP address and MAC address exist in the static ARP Inspection list. If the addresses match, the packet passes through the interface.
- If the device does not find a matching IP address, but DHCP Snooping is enabled on the VLAN, the device checks the DHCP Snooping database for the IP address-VLAN match. If the entry exists in the DHCP Snooping database, the packet passes through the interface.
- If the packet's IP address is not listed in the ARP Inspection List or the DHCP Snooping database, the device rejects the packet.



#### NOTE

To define ARP Inspection on VLANs, ARP Inspection List(s) must be defined before continuing.

In the following example, the List Name field is empty on the Add VLAN Settings page. If you add a list in the steps above, then the list will be populated with all the entries.

To define ARP Inspection on VLANs:

- STEP 1** Click **Security > ARP Inspection > VLAN Settings**. The *ARP Inspection VLAN Settings Page* opens:

#### ARP Inspection VLAN Settings Page



The *ARP Inspection VLAN Settings Page* contains the following fields:

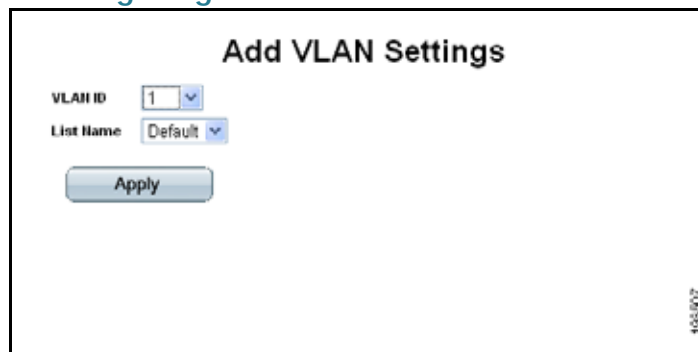
- **VLAN ID** — A user-defined VLAN ID to add to the Enabled VLANs list.
- **List Name** — Contains a list of VLANs in which ARP Inspection is enabled.

#### Enabled VLAN Table

- **VLAN ID**— Indicates the VLAN which is bound to the ARP Inspection List.
- **List Name** — Displays names of static ARP Inspection Lists that were assigned to VLANs. These lists are defined in the *ARP Inspection List Page*.

- STEP 2** Enter the name of a VLAN ID from the VLAN ID list and click **Add**. This VLAN ID then appears in the list. The *Add ARP VLAN Settings Page* opens:

#### Add ARP VLAN Settings Page



The *Add ARP VLAN Settings Page* contains the following fields:

- **VLAN ID** — Select the VLAN which includes the specified ARP Inspection List.
- **List Name** — Select a static ARP Inspection List to assign to the VLAN. These lists are defined in the *ARP Inspection List Page*.

**STEP 3** Define the fields.

**STEP 4** Click **Apply**. The new ARP VLAN configuration is defined, and the device is updated.

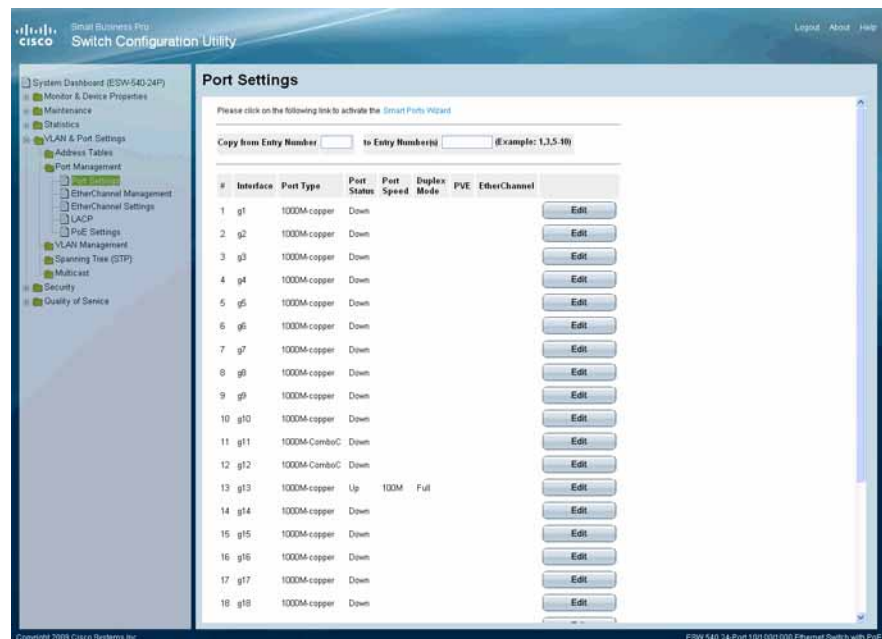
# Configuring Ports

## Port Settings

The Port Settings Page contains fields for defining port parameters. To define port settings:

- STEP 1** Click **VLAN & Port Settings > Port Management > Port Settings**. The *Port Settings Page* opens:

### Port Settings Page



The Port Settings Page contains the following fields:

- **Copy From Entry Number** — Copies the port configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied port configuration to the specified table entry.
- **Interface** — Displays the port number.

- **Port Type** — Displays the port type. The possible field values are:
  - *100M* — Copper
  - *1000M* — Copper (copper cable).
  - *1000M* — ComboC (combo port with copper cable 3).
  - *1000M* — ComboF (combo port with optic fiber cable).
  - *1000M FiberOptics* — Indicates the port has a fiber optic port connection.
- **Port Status** — Displays the port connection status. The possible field values are:
  - *Up* — Port is connected.
  - *Down* — Port is disconnected.
- **Port Speed** — Displays the current port speed.
- **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on EtherChannels. The possible field values are:
  - *Full* — Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
  - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **PVE** — Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it.
- **EtherChannel** — Defines if the port is part of a Link Aggregation Group (EtherChannel).

**STEP 2** To copy the settings from one interface to another, enter the specific interface numbers in the **Copy From Entry Number** and **To Entry Number(s)** fields.

**STEP 3** Click **Apply**. The Port Settings are defined, and the device is updated.

### Modifying Port Settings

**STEP 1** Click **VLAN & Port Settings > Port Management > Port Settings**. The *Port Settings Page* opens:

**STEP 2** Click a specific entry's **Edit** button. The *Edit Port Page* opens:

#### Edit Port Page

**Edit Port**

Port	g1
Description	
Port Type	1000M-copper
Admin Status	Up
Current Port Status	Down
Reactivate Suspended Port	<input type="checkbox"/>
Operational Status	Active
Admin Speed	1000M
Current Port Speed	
Admin Duplex	Full
Current Duplex Mode	
Auto Negotiation	Enable
Current Auto Negotiation	
Admin Advertisement	<input checked="" type="checkbox"/> Max Capability <input type="checkbox"/> 10 Half <input type="checkbox"/> 10 Full <input type="checkbox"/> 100 Half <input type="checkbox"/> 100 Full <input type="checkbox"/> 1000 Full
Current Advertisement	Unknown
Neighbor Advertisement	Unknown
Admin Back Pressure	Disable
Current Back Pressure	
Admin Flow Control	Disable
Current Flow Control	
Admin MDI/MDIX	AUTO
Current MDI/MDIX	
Ether Channel	
PVE	None

Apply

193610

The *Edit Port Page* contains the following fields:

- **Port** — Displays the port number.
- **Description** — Use this field to optionally define a name for the port.
- **Port Type** — Displays the port type. The possible field values are:

- *100M* — Copper
  - *1000M* — Copper (copper cable).
  - *1000M* — ComboC (combo port with copper cable 3).
  - *1000M* — ComboF (combo port with optic fiber cable).
  - *1000M FiberOptics* — Indicates the port has a fiber optic port connection.
- **Admin Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
  - Up — Indicates the port is currently operating.
  - Down — Indicates the port is currently not operating.
- **Current Port Status** — Displays the port connection status.
- **Reactivate Suspended Port** — Reactivates a port if the port has been disabled through the locked port security option or through Access Control List configurations.
- **Operational Status** — Indicates whether the port is currently active or inactive.
- **Admin Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. You can designate Admin Speed only when the port auto-negotiation is disabled.
- **Current Port Speed** — Displays the current port speed.
- **Admin Duplex** — Defines the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on EtherChannels. The possible field values are:
  - *Full* — Indicates that the interface supports transmission between the device and the client in both directions simultaneously.
  - *Half* — Indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — Displays the port current duplex mode.
- **Auto Negotiation** — Enables or Disables Auto Negotiation on the port. Auto Negotiation enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the Auto Negotiation status on the port.



- **Admin Advertisement** — Specifies the capabilities to be advertised by the Port. The possible field values are:
  - *Max Capability* — Indicates that all port speeds and Duplex mode settings can be accepted.
  - *10 Half* — Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.
  - *10 Full* — Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.
  - *100 Half* — Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.
  - *100 Full* — Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.
  - *1000 Full* — Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** — The port advertises its capabilities to its neighbor port to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — Displays the neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the Admin Advertisement field.
- **Admin Back Pressure** — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. The Back Pressure mode is configured for ports currently in the Half Duplex mode.
- **Current Back Pressure** — Displays the Back Pressure mode on the port.
- **Admin Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the port. Select from Enable, Disable, Auto-Negotiation.
- **Current Flow Control** — Displays the current Flow Control setting. Select from Enable, Disable, Auto-Negotiation.
- **Admin MDI/MDIX** — Displays the Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX) status on the port. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through

Ethernet cable can be used, and the pairs are matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to ensure that the correct pairs are connected. The possible field values are:

- *MDIX* — Use for hubs and switches.
- *Auto* — Use to automatically detect the cable type.
- *MDI* — Use for end stations.
- **Current MDI/MDIX** — Displays the current MDI/MDIX setting.
- **EtherChannel** — Defines if the port is part of a Link Aggregation Group (EtherChannel).
- **PVE** — Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it.

**STEP 3** Make the appropriate selections and click **Apply**. The device is updated.

---

# Configuring VLANs

VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, or through any other logical connection combination, since they are software-based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router working at a protocol level is required to allow traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are Broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packets belong. VLAN tags are attached to the VLAN by either the end station or the network device. VLAN tags also contain VLAN network priority information.

Combining VLANs and Generic Attribute Registration Protocol (GARP) allows network managers to define network nodes into Broadcast domains. The VLAN Management section contains the following topics:

This section contains the following topics:

- Defining VLAN Properties
- Defining VLAN Membership
- Assigning Ports to Multiple VLANs
- Defining Interface Settings
- Defining GVRP Settings
- Defining Protocol Groups
- Defining a Protocol Port

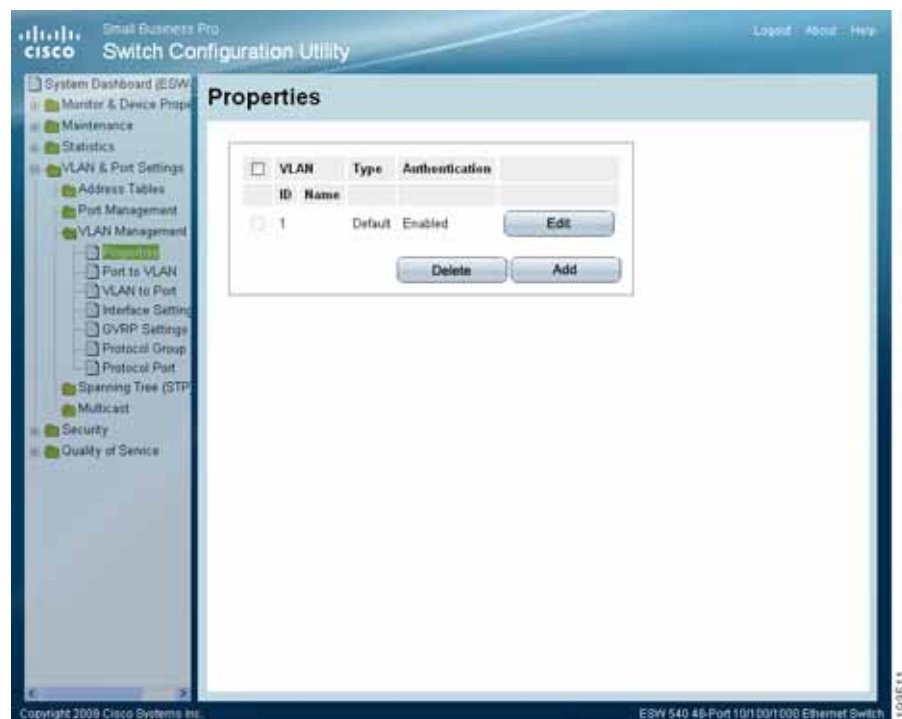
## Defining VLAN Properties

The *VLAN Properties Page* provides information and global parameters for configuring and working with VLANs.

To define VLAN properties:

- STEP 1** Click **VLAN & Port Settings > VLAN Management > Properties**. The *VLAN Properties Page* opens.

### VLAN Properties Page



The *VLAN Properties Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Displays the user-defined VLAN name.
- **Type** — Displays the VLAN type. The possible field values are:
  - *Dynamic* — Indicates the VLAN was dynamically created through GVRP.
  - *Static* — Indicates the VLAN is user-defined.
  - *Default* — Indicates the VLAN is the default VLAN.

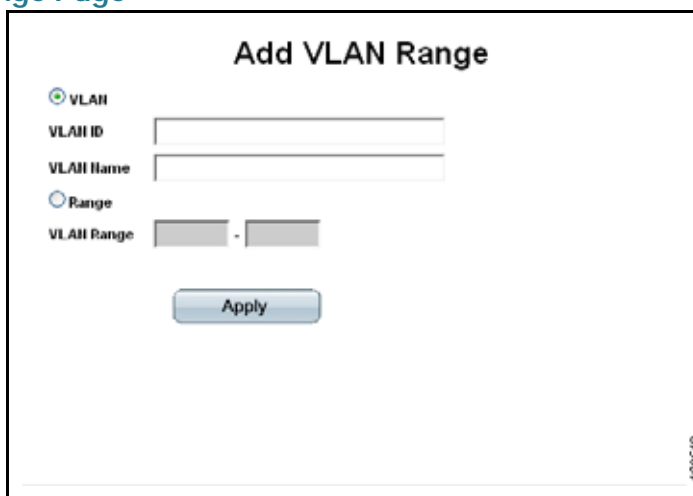
## Configuring VLANs

### Defining VLAN Properties

- **Authentication** — Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
  - *Enable* — Enables unauthorized users to use the Guest VLAN.
  - *Disable* — Disables unauthorized users from using the Guest VLAN.

**STEP 2** Click the **Add** button. The *Add VLAN Range Page* opens:

#### Add VLAN Range Page

The screenshot shows a web interface titled "Add VLAN Range". It contains two radio buttons: "VLAN" (which is selected) and "Range". Below the "VLAN" radio button are two text input fields labeled "VLAN ID" and "VLAN Name". Below the "Range" radio button are two text input fields labeled "VLAN Range" separated by a hyphen. At the bottom of the form is a blue "Apply" button. The page has a light gray background and a thin border.

The *Add VLAN Range Page* allows network administrators to define and configure new VLANs, and contains the following fields:

- **VLAN** — Specifies that a specific VLAN is to be defined. The possible field values are:
  - **VLAN ID** — Defines the VLAN ID.
  - **VLAN Name** — Defines a VLAN name.
- **Range** — Specifies that a range of VLAN IDs is to be defined. The possible field values are:
  - **VLAN Range** — Defines the lower and upper bounds of the VLAN range.

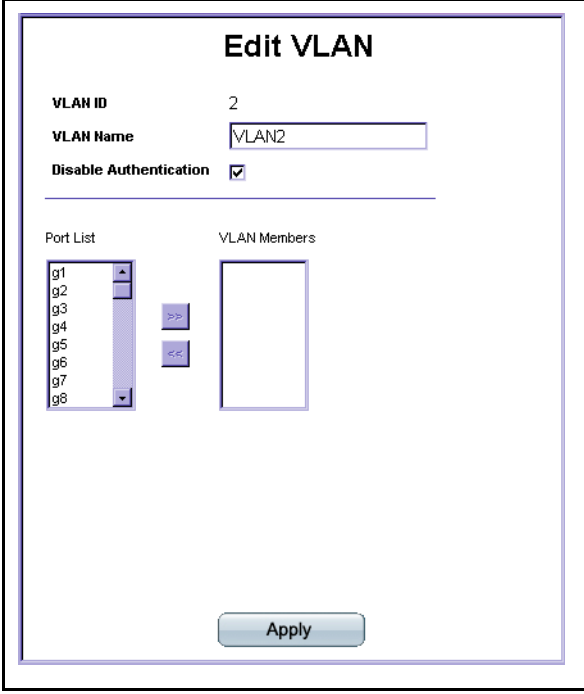
**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The VLAN Settings are defined, and the device is updated.

## Modifying VLANs

- STEP 1** Click **VLAN & Port Settings > VLAN Management > Properties**. The *VLAN Properties Page* opens.
- STEP 2** Click **Edit**. The *Edit VLAN Page* opens:

### Edit VLAN Page



The screenshot shows the 'Edit VLAN' configuration page. At the top, the title 'Edit VLAN' is centered. Below it, there are three fields: 'VLAN ID' with the value '2', 'VLAN Name' with the value 'VLAN2', and 'Disable Authentication' which is checked. Below these fields, there are two sections: 'Port List' and 'VLAN Members'. The 'Port List' section contains a list of ports from g1 to g8. The 'VLAN Members' section is currently empty. Between the two sections are two buttons: '>>' and '<<'. At the bottom of the page is an 'Apply' button.

The *Edit VLAN Page* contains information for enabling VLAN guest authentication, and includes the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Defines the VLAN name.
- **Disable Authentication** — Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:
  - *Checked* — Enables unauthorized users to use the Guest VLAN.
  - *Unchecked* — Disables unauthorized users from using the Guest VLAN.
- **Port List** — Available ports on the device. Select ports from this list to include in the VLAN.
- **VLAN Members** — Ports included in the VLAN.

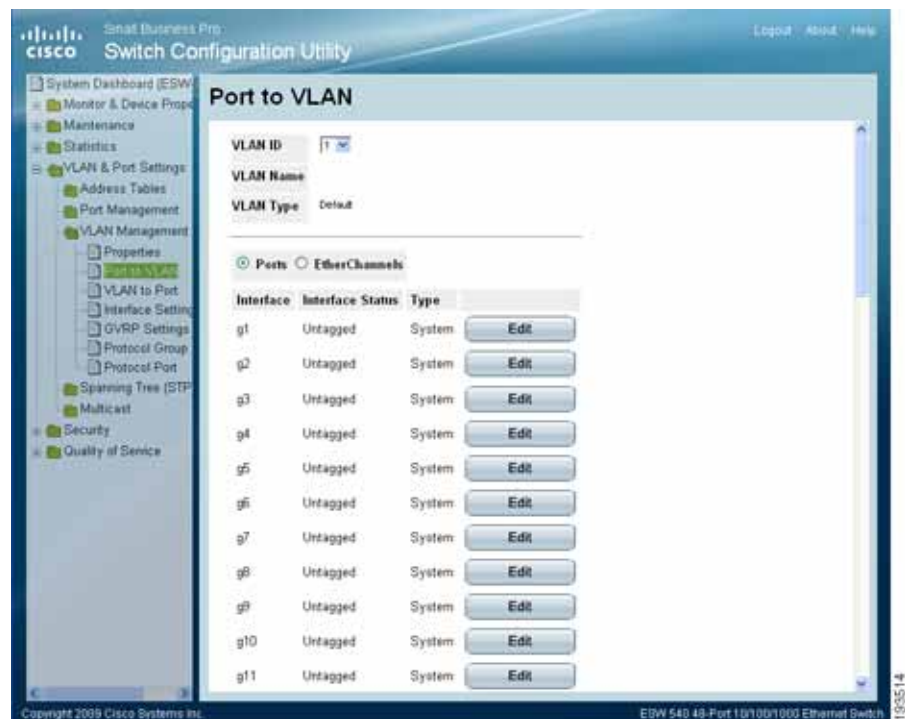
- STEP 3** Define the relevant fields.
- STEP 4** In the Port List, select the ports to include in the VLAN and click the adjacent right arrow. The selected ports then appear in the VLAN Members list.
- STEP 5** Click **Apply**. The VLAN Settings are defined, and the device is updated.

## Defining VLAN Membership

The *Port to VLAN Page* contains a table that maps VLAN parameters to ports. Ports are assigned VLAN membership by toggling through the Port Control settings.

- STEP 1** Click **VLAN & Port Settings > VLAN Management > Port to VLAN**. The *Port to VLAN Page* opens:

### Port to VLAN Page



The *Port to VLAN Page* contains the following fields:

- **VLAN ID** — Selects the VLAN ID.

- **VLAN Name** — Displays the VLAN name.
- **VLAN Type** — Indicates the VLAN type. The possible field values are:
  - *Dynamic* — Indicates the VLAN was dynamically created through GVRP.
  - *Static* — Indicates the VLAN is user-defined.
  - *Default* — Indicates the VLAN is the default VLAN.
- **Ports** — Indicates that ports are described in the page.
- **EtherChannels** — Indicates that EtherChannels are described in the page.
- **Interface** — Displays the interface configuration being displayed.
- **Interface Status** — Indicates the interface's membership status in the VLAN. The possible field values are:
  - *Untagged* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
  - *Tagged* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
  - *Exclude* — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
  - *Forbidden* — Denies the interface VLAN membership, even if GARP indicates the port is to be added.

**STEP 2** Select VLAN ID from drop-down list and then EDIT ports.

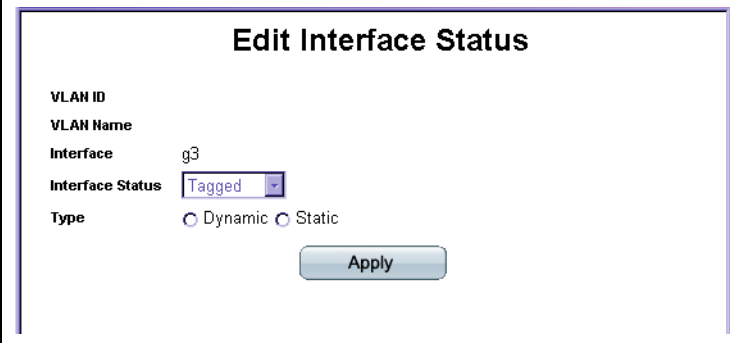
### Modifying VLAN Membership

**STEP 3** Click **VLAN & Port Settings > VLAN Management > Port to VLAN**. The *Port to VLAN Page* opens:

**STEP 4** Click the **Edit** button. The *Edit Interface Status Page* opens:



### Edit Interface Status Page



The screenshot shows a web-based configuration page titled "Edit Interface Status". It contains the following fields and controls:

- VLAN ID**: A text field.
- VLAN Name**: A text field.
- Interface**: A text field containing the value "g3".
- Interface Status**: A dropdown menu currently set to "Tagged".
- Type**: Two radio buttons labeled "Dynamic" and "Static".
- Apply**: A button at the bottom right of the form.

The *Edit Interface Status Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **VLAN Name** — Displays the VLAN name.
- **Interface** — Defines the port or EtherChannel attached to the VLAN.
- **Interface Status** — Defines the current interface's membership status in the VLAN. The possible field values are:
  - *Untagged* — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
  - *Tagged* — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
  - *Exclude* — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
  - *Forbidden* — Denies the interface VLAN membership, even if GARP indicates the port is to be added.
- **Type** — Indicates the VLAN type, Dynamic indicates the VLAN was dynamically created through GARP, Static indicates the VLAN is user defined.

**STEP 5** Define the relevant fields.

**STEP 6** Click **Apply**. VLAN Membership is modified, and the device is updated.

## Assigning Ports to Multiple VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

**Note:** VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

The *VLAN To Port Page* contains fields for configuring VLANs to ports. The network administrator allows the user to assign a single port to multiple VLANs.

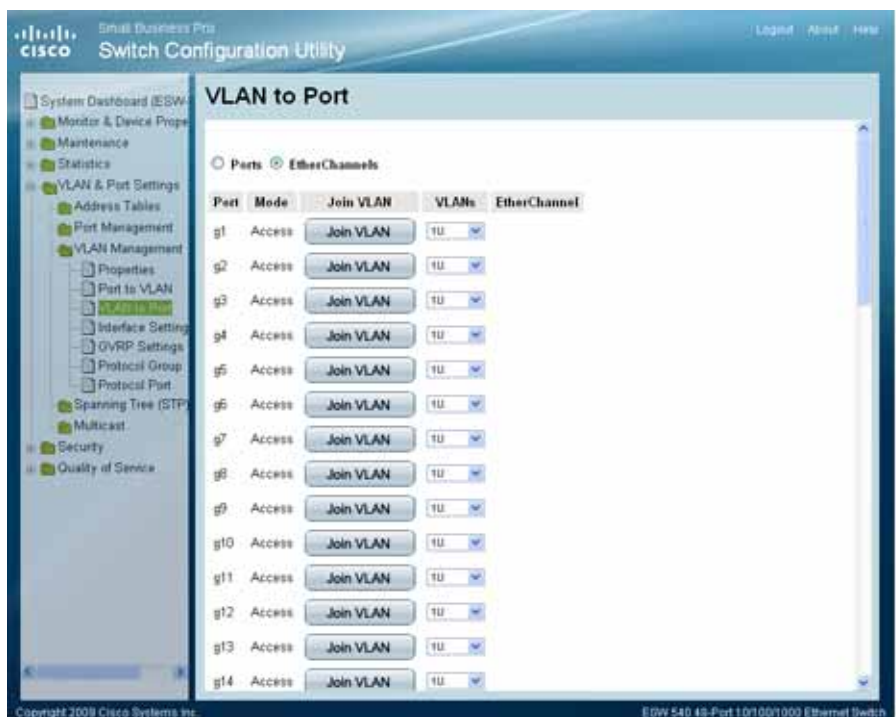
To add VLAN membership to a port:

## Configuring VLANs

### Assigning Ports to Multiple VLANs

- STEP 1** Click **VLAN & Port Settings > VLAN Management > VLAN to Port**. The *VLAN To Port Page* opens:

#### VLAN To Port Page



The *VLAN To Port Page* contains the following fields:

- **Ports** — Indicates that ports are described in the page.
- **EtherChannels** — Indicates that EtherChannels are described in the page.
- **Port** — Displays the port number.
- **Mode** — Indicates the port mode. The possible values are:
  - *General* — Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode).
  - *Access* — Indicates a port belongs to a single untagged VLAN.
  - *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged.
  - *Customer* — The port belongs to a VLAN in which all ports are untagged.

## Configuring VLANs

### Assigning Ports to Multiple VLANs

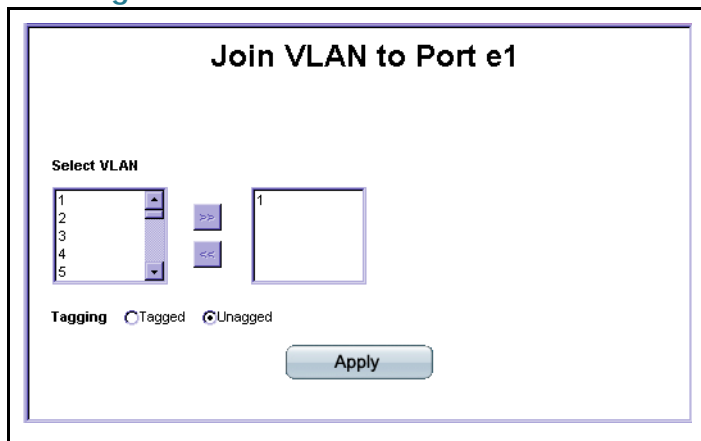
- **Join VLAN** — Defines the VLANs to which the interface is joined. Pressing the Join VLAN button displays the *Join VLAN to Port Page*.

Select the VLAN to which to add the port, select the VLANs to be tagged or untagged and click >>. To remove the VLAN allocation to the port, select the VLAN already assigned to the port and click <<.

- **VLANs** — Specifies the VLAN in which the port is a member.
- **EtherChannel** — if the port is a member of an EtherChannel, the EtherChannel number is displayed. A member of an EtherChannel cannot be configured to a VLAN, but that same EtherChannel can be configured to a VLAN.

**STEP 2** In the *VLAN To Port* table, click **Join VLAN** in the relevant port entry. The *Join VLAN To Port Page* opens.

#### Join VLAN To Port Page



**STEP 3** Define the selected VLAN as *Tagged* or *Untagged*.

**STEP 4** From the left list, select the relevant VLAN and click >>. The selected VLAN then appears in the right list. Up to 20 VLANs at a single time may be joined to the port.

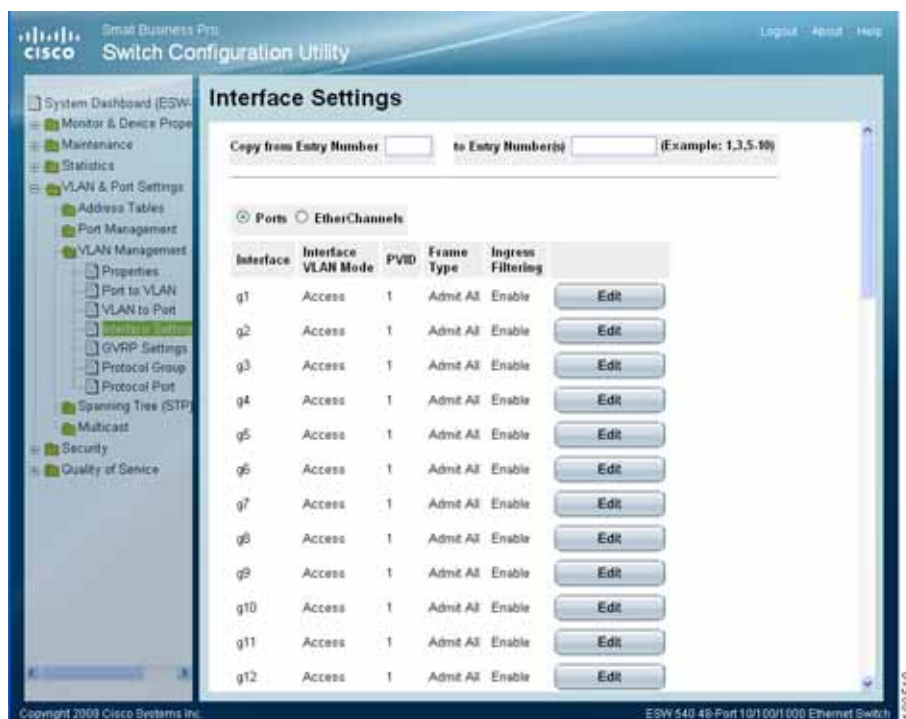
**STEP 5** Click **Apply**. VLAN to Port setting is defined, and the device is updated.

## Defining Interface Settings

The *VLAN Interface Setting Page* provides parameters for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the *VLAN Port Settings* page. All untagged packets arriving to the device are tagged by the ports PVID.

**STEP 1** Click **VLAN & Port Settings > VLAN Management > Interface Settings**. The *VLAN Interface Settings Page* opens:

### VLAN Interface Setting Page



The *VLAN Interface Setting Page* contains the following fields:

- **Copy From Entry Number** — Copies VLAN configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied VLAN configuration to the specified table entry.
- **Ports** — Indicates that ports are described in the page.
- **EtherChannels** — Indicates that EtherChannels are described in the page.

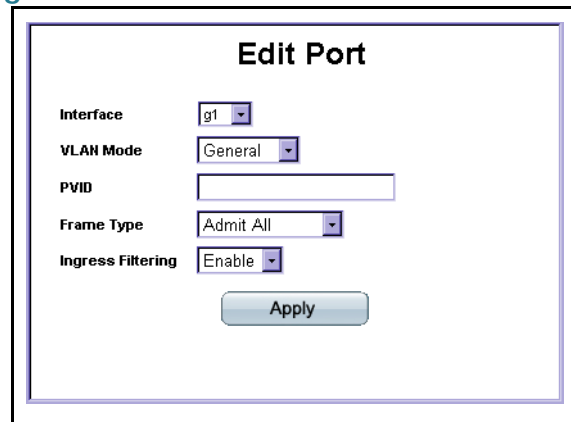
- **Interface** — The port number included in the VLAN.
- **Interface VLAN Mode** — Indicates the port mode. Possible values are:
  - *General* — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - *Access* — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.
  - *Trunk* — The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).
  - *Customer* — The port belongs to VLANs. In Customer mode, the added tag provides a VLAN ID to each customer, ensuring private and segregated network traffic.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1 to 4095. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Packet type accepted on the port. Possible values are:
  - *Admit Tag Only* — Indicates that only tagged packets are accepted on the port.
  - *Admit All* — Indicates that both tagged and untagged packets are accepted on the port.
- **Ingress Filtering** — Ingress filtering discards packets which do not include an ingress port. The possible values are:
  - *Enable* — Ingress filtering is activated on the port.
  - *Disable* — Ingress filtering is not activated on the port.

## Modifying VLAN Interface Settings

**STEP 2** Click **VLAN & Port Settings > VLAN Management > Interface Settings**. The *VLAN Interface Settings Page* opens:

**STEP 3** Click the **Edit** button. The *Edit VLAN Port Page* opens:

### Edit VLAN Port Page

The screenshot shows a web-based configuration page titled "Edit Port". It contains several fields for configuring a port: "Interface" is a dropdown menu with "g1" selected; "VLAN Mode" is a dropdown menu with "General" selected; "PVID" is a text input field; "Frame Type" is a dropdown menu with "Admit All" selected; and "Ingress Filtering" is a dropdown menu with "Enable" selected. Below these fields is an "Apply" button.

The *Edit VLAN Port Page* contains the following fields:

- **Interface** — The port or EtherChannel associated with this VLAN interface configuration.
- **VLAN Mode** — Indicates the port mode. Possible values are:
  - *General* — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
  - *Access* — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.
  - *Trunk* — The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).
  - *Customer* — The port belongs to VLANs. In Customer mode, the added tag provides a VLAN ID to each customer, ensuring private and segregated network traffic.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1 to 4095. Packets classified to the Discard VLAN are dropped.
- **Frame Type** — Packet type accepted on the port. Possible values are:
  - *Admit Tag Only* — Indicates that only tagged packets are accepted on the port.
  - *Admit All* — Indicates that both tagged and untagged packets are accepted on the port.

- **Ingress Filtering** — Ingress filtering discards packets which do not include an ingress port. The possible values are:
  - *Enable* — Ingress filtering is activated on the port.
  - *Disable* — Ingress filtering is not activated on the port.

**STEP 4** Define the relevant fields.

**STEP 5** Click **Apply**. The VLAN Interface settings are modified, and the device is updated.

## Defining GVRP Settings

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

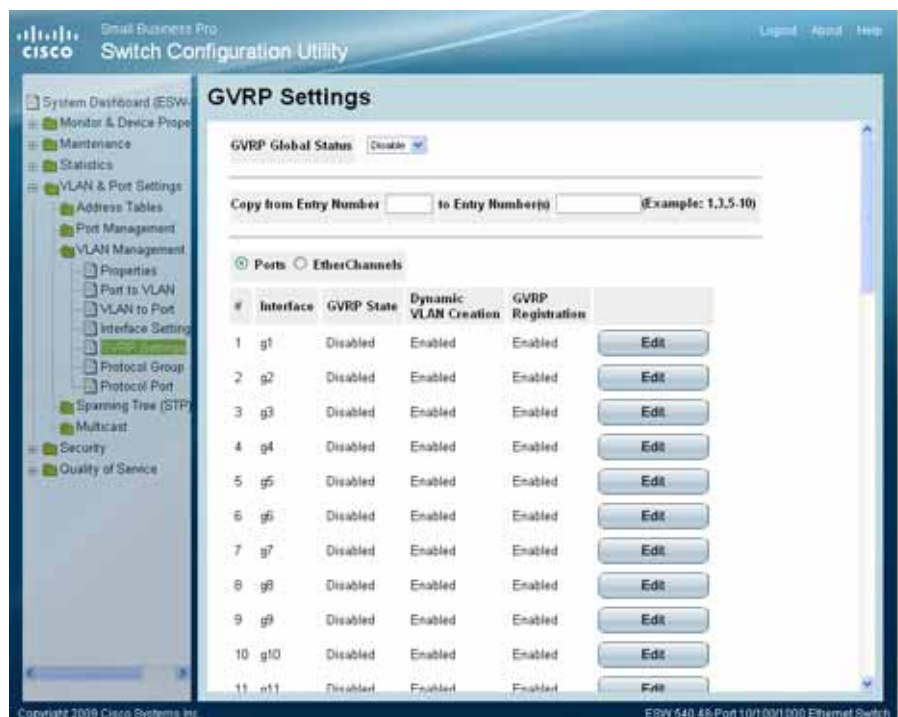
The Global System EtherChannel information displays the same field information as the ports, but represents the EtherChannel GVRP information.

To define GVRP:



**STEP 1** Click **VLAN & Port Settings > VLAN Management > GVRP Settings**. The *GVRP Settings Page* opens:

#### GVRP Settings Page



The *GVRP Settings Page* contains the following fields:

- **GVRP Global Status** — Indicates if GVRP is enabled on the device. The possible field values are:
  - *Enable* — Enables GVRP on the device.
  - *Disable* — Disables GVRP on the device.
- **Copy From Entry Number** — Copies GVRP parameters from the specified table entry.
- **To Entry Number(s)** — Assigns the copied GVRP parameters to the specified table entry.
- **Ports** — Indicates that ports are described on the page.
- **EtherChannels** — Indicates that EtherChannels are described on the page.
- **Interface** — Interface described by the GVRP settings entry.

- **GVRP State** — Indicates if GVRP is enabled on the interface. The possible field values are:
  - *Enabled* — Enables GVRP on the selected interface.
  - *Disabled* — Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  - *Enabled* — Enables Dynamic VLAN creation on the interface.
  - *Disabled* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
  - *Enabled* — Enables GVRP registration on the device.
  - *Disabled* — Disables GVRP registration on the device.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The GVRP Settings are defined, and the device is updated.

---

## Modifying GVRP Settings

**STEP 1** Click **VLAN & Port Settings > VLAN Management > GVRP Settings**. The *GVRP Settings Page* opens:

**STEP 2** Click the **Edit** button. The *Edit GVRP Page* opens:

### Edit GVRP Page

**Edit GVRP**

Interface ☒ Port ☐ EtherChannel  
GVRP State  
Dynamic VLAN Creation  
GVRP Registration  
Apply

The *Edit GVRP Page* contains the following fields:

- **Interface** — Port or EtherChannel described by the GVRP settings entry.
- **GVRP State** — Indicates if GVRP is enabled on the interface. The possible field values are:
  - *Enable* — Enables GVRP on the selected interface.
  - *Disable* — Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  - *Enable* — Enables Dynamic VLAN creation on the interface.
  - *Disable* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
  - *Enable* — Enables GVRP registration on the device.
  - *Disable* — Disables GVRP registration on the device.

**STEP 3** Define the relevant fields.

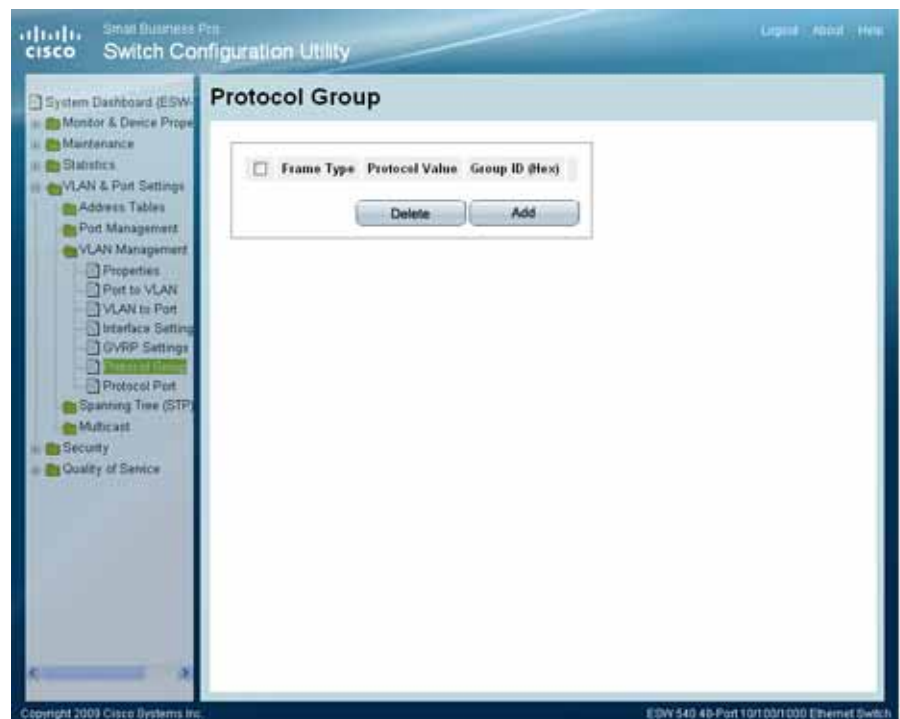
**STEP 4** Click **Apply**. GVRP settings are modified, and the device is updated.

## Defining Protocol Groups

The *Protocol Group Page* contains information which describes the protocol names and the VLAN Ethernet type. Interfaces can be classified as a specific protocol based interface.

- STEP 1** Click **VLAN & Port Settings > VLAN Management > Protocol Group**. The *Protocol Group Page* opens:

### Protocol Group Page

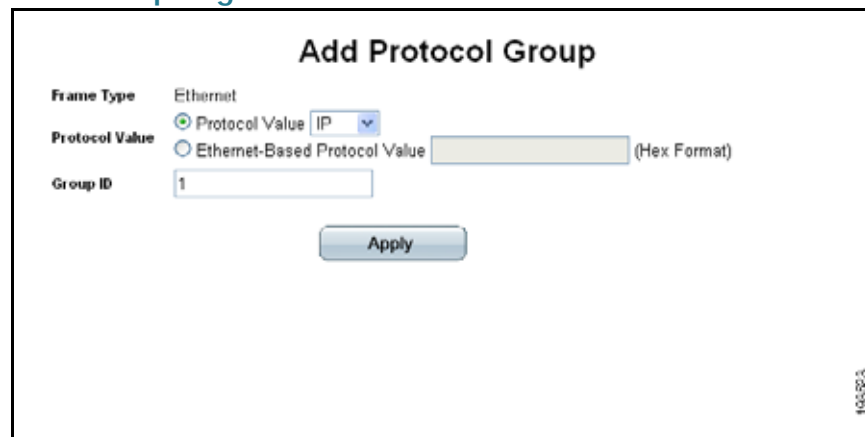


The *Protocol Group Page* contains the following fields:

- **Frame Type** — Displays the packet type.
- **Protocol Value** — Displays the User-defined protocol name.
- **Group ID (Hex)** — Defines the Protocol group ID to which the interface is added. Range is 1-2147483647.

- STEP 2** Click the **Add** Button. The *Add Protocol Group Page* opens:

#### Add Protocol Group Page



The screenshot shows the 'Add Protocol Group' configuration page. It includes the following fields and options:

- Frame Type:** A dropdown menu set to 'Ethernet'.
- Protocol Value:** Two radio button options: 'Protocol Value' (selected) and 'Ethernet-Based Protocol Value'. The 'Protocol Value' option has a dropdown menu set to 'IP'. The 'Ethernet-Based Protocol Value' option has a text input field followed by '(Hex Format)'.
- Group ID:** A text input field containing the value '1'.
- Apply:** A button at the bottom center of the form.

A vertical label '105823' is visible on the right side of the form.

The *Add Protocol Group Page* provides information for configuring new VLAN protocol groups. The *Add Protocol Group Page* contains the following fields.

- **Frame Type** — Displays the packet type.
- **Protocol Value** — Defines the User-defined protocol value. The options are as follows:
  - *Protocol Value* — The possible values are IP, IPX, or ARP.
  - *Ethernet-Based Protocol Value* — Specify the value in hexadecimal format.
- **Group ID** — Defines the Protocol group ID to which the interface is added. The possible value range is 1-2147483647 in hexadecimal format.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Protocol Group is added, and the device is updated.


## Modifying Protocol Groups

The *Edit Protocol Group Page* provides information for configuring existing VLAN protocol groups

**STEP 1** Click **VLAN & Port Settings > VLAN Management > Protocol Group**. The *Protocol Group Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit Protocol Group Page* opens:

#### Edit Protocol Group Page



The screenshot shows a web interface titled "Edit Protocol Group". It contains three configuration fields: "Frame Type" set to "Ethernet", "Protocol Value" set to "a1b1", and "Group ID (Hex)" with a text input field containing the value "1". Below these fields is a blue "Apply" button.

The *Edit Protocol Group Page* contains the following fields.

- **Frame Type** — Displays the packet type.
- **Protocol Value** — Displays the User-defined protocol value.
- **Group ID (Hex)** — Defines the Protocol group ID to which the interface is added. The possible value range is 1-2147483647 in hexadecimal format.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Protocol group is modified, and the device is updated.

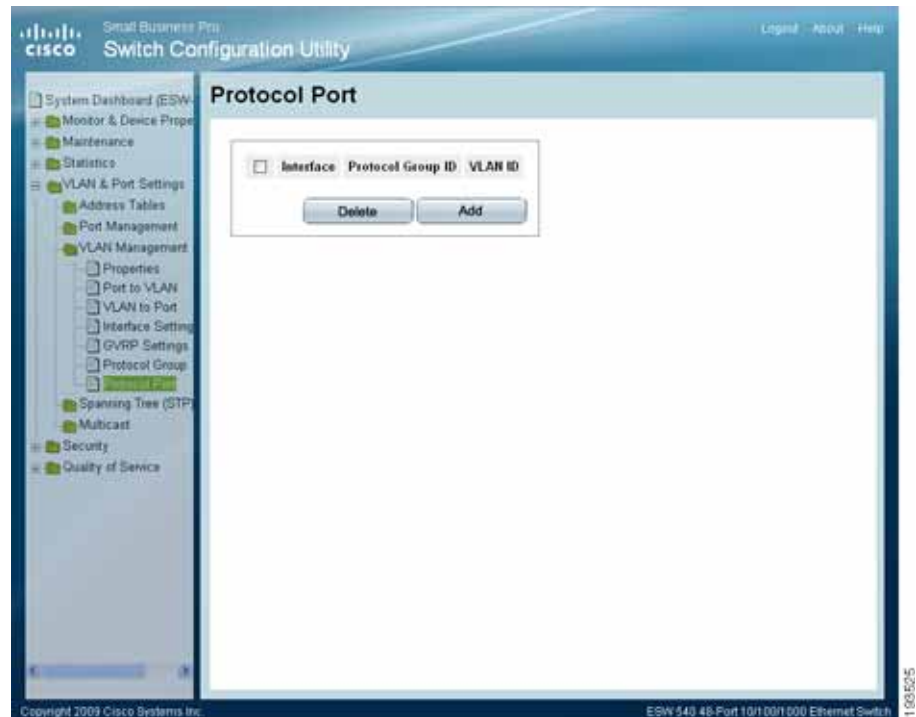
## Defining a Protocol Port

The *Protocol Port Page* adds interfaces to Protocol groups.

To define the protocol port:

- STEP 1** Click **VLAN & Port Settings > VLAN Management > Protocol Port**. The *Protocol Port Page* opens:

#### Protocol Port Page



The *Protocol Port Page* contains the following fields.

- **Interface** — Port or EtherChannel number added to a protocol group.
- **Protocol Group ID** — Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- **VLAN ID** — Attaches the interface to a user-defined VLAN ID. Protocol ports can either be attached to a VLAN ID or a VLAN name.

- STEP 2** Click the **Add** Button. The *Add Protocol Port to VLAN Page* opens:

The *Add Protocol Port to VLAN Page* provides parameters for adding protocol port configurations.

#### Add Protocol Port to VLAN Page

**Add Protocol Port to VLAN**

Interface ☒ Port ☐ EtherChannel  
Group ID  
VLAN ID ☒ 1  
VLAN Name ☐

The *Add Protocol Port to VLAN Page* contains the following fields.

- **Interface** — Port or EtherChannel number added to a protocol group.
- **Group ID** — Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- **VLAN ID** — Attaches the interface to a user-defined VLAN ID.
- **VLAN Name** — Attaches the interface to a user-defined VLAN Name.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The protocol ports are mapped to VLANs, and the device is updated.



# Configuring IP Information

The IP address and default gateway can be either dynamically or statically configured. In Layer 2, a static IP address is configured on the IPv4 Interface Page. The Management VLAN is set to VLAN 1 by default, but can be modified.

This section provides information for defining device IP addresses, and includes the following topics:

- IP Addressing
- Defining DHCP Relay
- Defining DHCP Relay Interfaces
- ARP
- Domain Name System

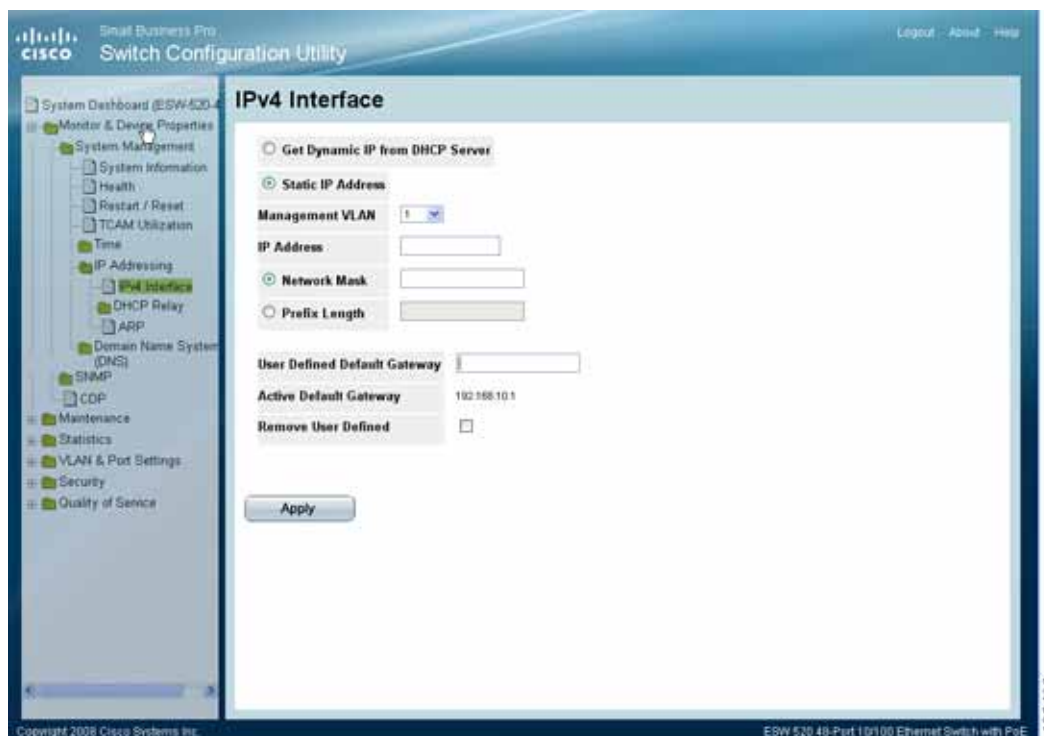
## IP Addressing

The IP address and default gateway can be either dynamically or statically configured. In Layer 2, a static IP address is configured on the *IPv4 Interface Page*. The Management VLAN is set to VLAN 1 by default, but can be modified.

The *IPv4 Interface Page* contains fields for assigning IPv4 addresses. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces.

- STEP 1** Click **Monitor & Device Properties > System Management > IP Addressing > IPv4 Interface**. The *IPv4 Interface Page* opens:

#### IPv4 Interface Page



The *IPv4 Interface Page* contains the following fields:

- **Get Dynamic IP from DHCP Server** — Retrieves the IP addresses using DHCP.
- **Static IP Address** — Permanent IP addresses are defined by the administrator. IP addresses are either configured on the Default VLAN or are user-defined.
- **Management VLAN** — Sets the management VLAN. The switch uses this VLAN to watch for management packets from Telnet and web browser management sessions. Management VLAN is set to 1 or 100 by default.
- **IP Address** — The currently configured IP address.
- **Network Mask** — Displays the currently configured IP address mask.
- **Prefix Length** — Specifies the prefix length. The range is 5 -128 (64 in the case EUI-64 parameter is used).
- **User Defined Default Gateway** — Manually defined default gateway IP address.

- **Active Default Gateway** — Active default gateway's IP Address.
- **Remove User Defined** — Removes the selected IP address from the interface. The possible field values are:
  - *Checked* — Removes the IP address from the interface.
  - *Unchecked* — Maintains the IP address assigned to the Interface.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The IP information is defined, and the device is updated.

## Defining DHCP Relay

The *DHCP Server Page* enables users to establish a DHCP configuration with multiple DHCP servers to ensure redundancy.

The DHCP servers act as a DHCP relay if the parameter is not equal to 0.0.0.0. DHCP requests are relayed only if their SEC field is greater or equal to the threshold value. This allows local DHCP Servers to respond first.

To define the DHCP Relay configuration:

## Configuring IP Information

### Defining DHCP Relay

- STEP 1** Click **Monitor & Device Properties > System Management > IP Addressing > DHCP Relay > DHCP Server**. The *DHCP Server Page* opens:

#### DHCP Server Page

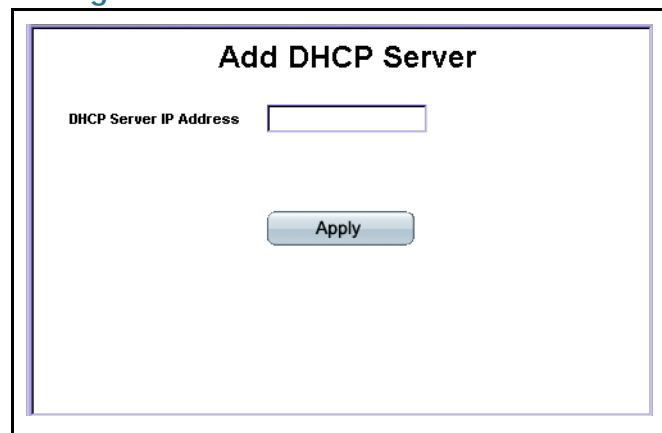


The *DHCP Server Page* Server contains the following fields:

- **DHCP Relay** — Enable or disable DHCP Server on the device. The possible values are:
  - *Enable* — Enables DHCP Relay on the device.
  - *Disable* — Disables DHCP Relay on the device.
- **Option 82** — Indicates if Option 82 is enabled for DHCP. The possible values are:
  - *Enable* — Enables Option 82 for DHCP.
  - *Disable* — Disables Option 82 for DHCP.
- **DHCP Server** — Display the IP address of the DHCP server.

- STEP 2** Click the **Add** button. The *Add DHCP Server Page* opens:

#### Add DHCP Server Page

The screenshot shows a web-based configuration page titled "Add DHCP Server". Inside a rectangular frame, there is a label "DHCP Server IP Address" followed by a text input field. Below the input field is a button labeled "Apply".

The *Add DHCP Server Page* contains the following field:

- **DHCP Server IP Address** — Defines the IP address assigned to the DHCP server.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The DHCP Server is defined, and the device is updated.

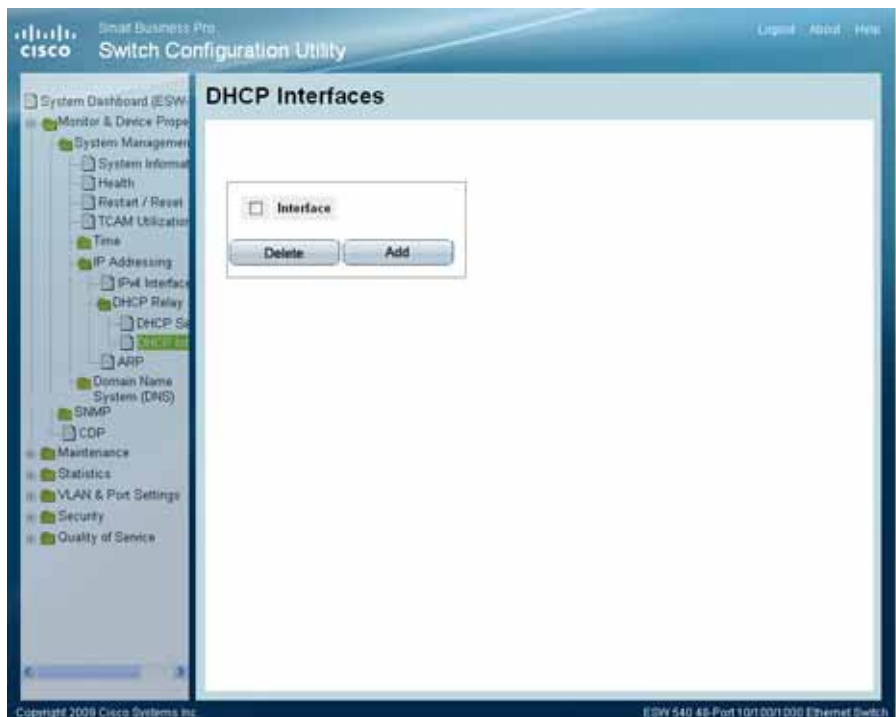
## Defining DHCP Relay Interfaces

Enabling Relay functionality provides multiple interfaces to be configured for establishing a DHCP Configuration with multiple DHCP servers to ensure redundancy. IP Addresses are controlled and distributed one-by-one to avoid storming the device.

To define the DHCP Relay configuration:

- STEP 1** Click **Monitor & Device Properties > System Management > IP Addressing > DHCP Relay > DHCP Interfaces**. The *DHCP Interfaces Page* opens:

#### DHCP Interfaces Page

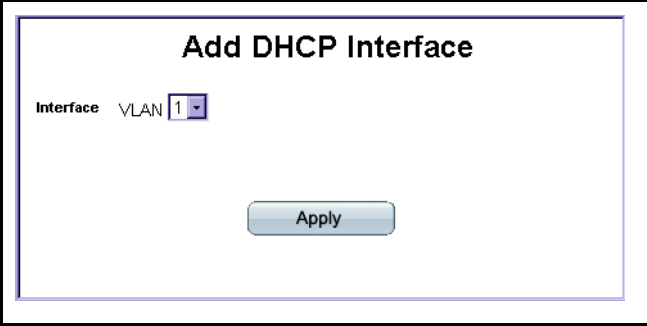


The *DHCP Interfaces Page* contains the following fields:

- **Check Box** — Removes DHCP relay from an interface. The possible field values are:
  - *Checked* — Check this box and press Delete to remove the selected DHCP Relay interface.
  - *Unchecked* — Maintains the selected DHCP Relay interface.
- **Interface** — Displays the interface selected for relay functionality.

- STEP 2** Click the **Add** button. The *Add DHCP Interface Page* opens:

#### Add DHCP Interface Page

The screenshot shows a web-based configuration page titled "Add DHCP Interface". Inside the page, there is a label "Interface" followed by a dropdown menu showing "VLAN 1". Below this, there is a blue "Apply" button.

**Add DHCP Interface**

Interface VLAN 1

Apply

The *Add DHCP Interface Page* contains the following field:

- **Interface** — Selects the interface to define DHCP Relay. The possible field value is:
  - *VLAN*— Defines the DHCP Relay on the selected VLAN.

**STEP 3** Select the Interface on which to define a DHCP Relay.

**STEP 4** Click **Apply**. A DHCP Relay Interface is defined, and the device is updated.

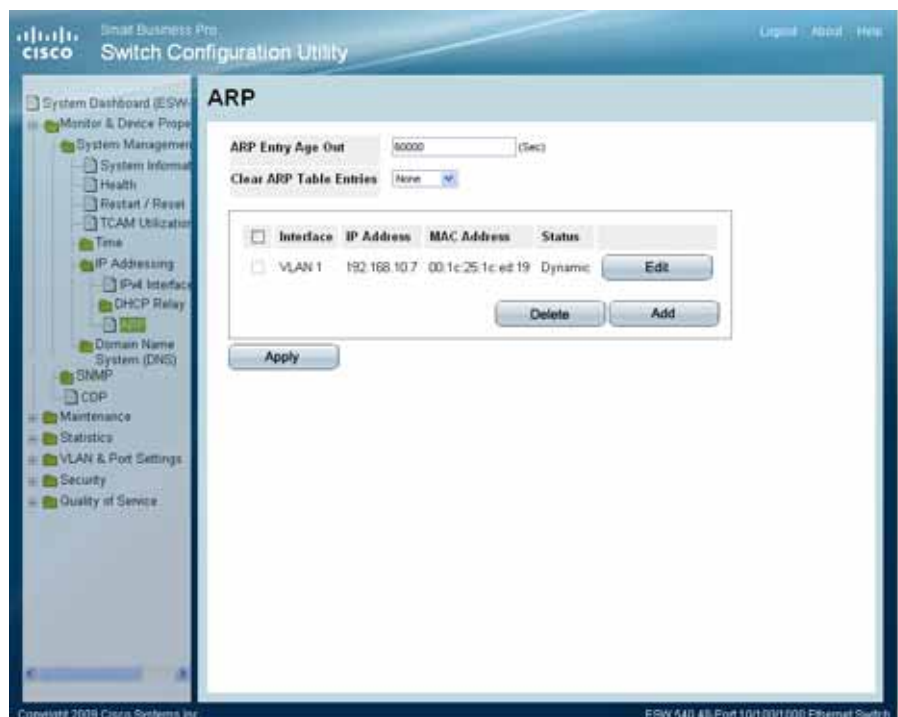
## Managing ARP

The *Address Resolution Protocol* (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. The ARP table is used to maintain a correlation between each MAC address and its corresponding IP address. The ARP table can be filled in statically by the user. When a static ARP entry is defined, a permanent entry is put in the table, which the system uses to translate IP addresses to MAC addresses.

To define ARP:

- STEP 1** Click **Monitor & Device Properties > System Management > IP Addressing > ARP**.  
The *ARP Page* opens:

#### ARP Page



The *ARP Page* contains the following fields.

- **ARP Entry Age Out** — Defines the amount of time (seconds) that pass between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is 1 - 40000000, where zero indicates that entries are never cleared from the cache. The default value is 60,000 seconds.
- **Clear ARP Table Entries** — Indicates the type of ARP entries that are cleared on all devices. The possible values are:
  - *None* — ARP entries are not cleared.
  - *All* — All ARP entries are cleared.
  - *Dynamic* — Only dynamic ARP entries are cleared.
  - *Static* — Only static ARP entries are cleared.




## ARP Table

- **Interface** — Indicates the interface for which the ARP parameters are defined.
- **IP Address** — Indicates the station IP address, which is associated with the MAC address.
- **MAC Address** — Indicates the station MAC address, which is associated in the ARP table with the IP address.
- **Status** — Indicates the ARP Table entry status. Possible field values are:
  - *Dynamic* — Indicates the ARP entry was learned dynamically.
  - *Static* — Indicates the ARP entry is a static entry.

**STEP 2** Click **Add**. The *Add ARP Page* opens:

### Add ARP Page



The *Add ARP Page* contains the following fields:

- **VLAN** — Indicates the ARP-enabled interface.
- **IP Address** — Indicates the station IP address, which is associated with the MAC address filled in below.
- **MAC Address** — Indicates the station MAC address, which is associated in the ARP table with the IP address.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The ARP Settings are defined, and the device is updated.

## Modifying ARP Settings

**STEP 1** Click **Monitor & Device Properties > System Management > IP Addressing > ARP**. The *ARP Page* opens:

**STEP 2** Click the **Edit** button. The *Edit ARP Page* opens:

### Edit ARP Page

The screenshot shows the 'Edit ARP' configuration window. It contains four labeled fields: 'VLAN' with the value '1', 'IP Address' with a dropdown menu showing '192.168.10.7', 'MAC Address' with a text box containing '00:1c:25:1c:ed:19', and 'Status' with a dropdown menu showing 'Dynamic'. Below these fields is an 'Apply' button. The window title is 'Edit ARP' and there is a small icon in the bottom right corner.

The *Edit ARP Page* contains the following fields:

- **VLAN** — Indicates the ARP-enabled interface.
- **IP Address** — Indicates the station IP address, which is associated with the MAC address filled in below.
- **MAC Address** — Indicates the station MAC address, which is associated in the ARP table with the IP address.
- **Status** — Defines the ARP Table entry status. Possible field values are:
  - *Dynamic* — Indicates the ARP entry is learned dynamically.
  - *Static* — Indicates the ARP entry is a static entry.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The ARP Settings are modified, and the device is updated.

# Domain Name System

*Domain Name System* (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address. For example, **www.ipexample.com** is translated into 192.87.56.2. DNS servers maintain databases of domain names and their corresponding IP addresses. The Domain Name System contains the following pages:

- Defining DNS Servers
- Mapping DNS Hosts

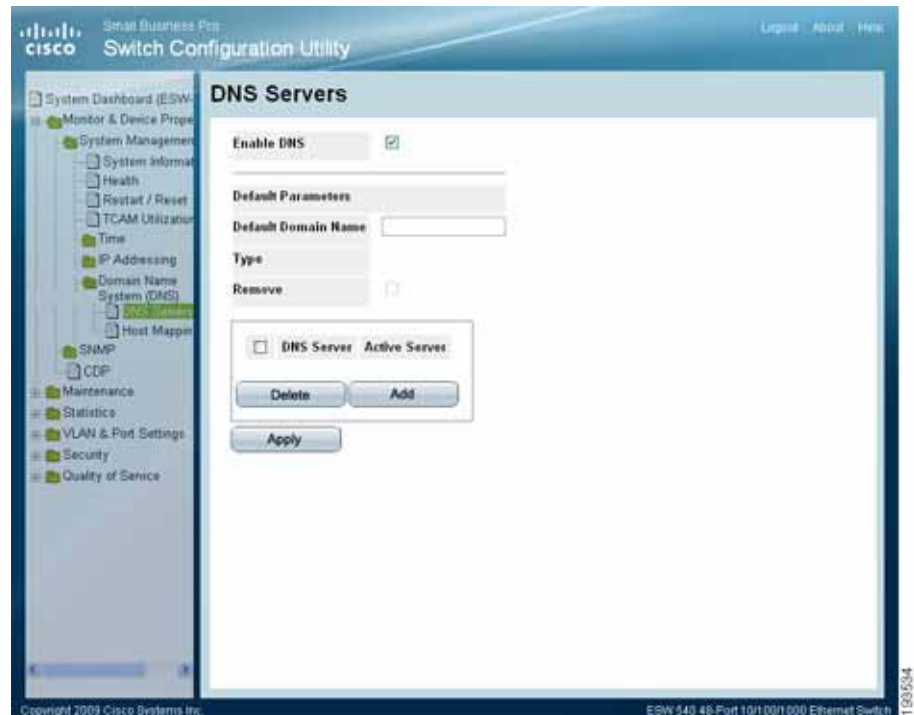
## Defining DNS Servers

The *DNS Servers Page* contains fields for enabling and activating specific DNS servers.

To enable a DNS client:

- STEP 1** Click **Monitor & Device Properties > System Management > Domain Name System (DNS) > DNS Servers**. The *DNS Servers Page* opens:

#### DNS Servers Page



The *DNS Servers Page* contains the following fields.

- **Enable DNS** — Enables translating the DNS names into IP addresses. The possible field values are:
  - *Checked* — Translates the domains into IP addresses.
  - *Unchecked* — Disables translating domains into IP addresses.

#### Default Parameters

- **Default Domain Name** — Specifies the user-defined DNS server name (1 -158 characters).
- **Type** — Displays the IP address type. The possible field values are:
  - *DHCP* — The IP address is dynamically created.
  - *Static* — The IP address is a static IP address.
- **Remove** — Removes DNS servers. The possible field values are:

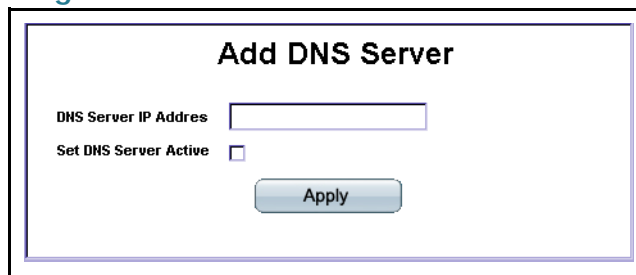
- *Checked*— Removes the selected DNS server
- *Unchecked*— Maintains the current DNS server list.

### DNS Server Details

- **DNS Server** — Displays the DNS server's IP address, up to four DNS servers can be defined.
- **Active Server** — Specifies the DNS server that is currently active.

**STEP 2** Click the **Add** button. The *Add DNS Server Page* opens:

### Add DNS Server Page



The *Add DNS Server Page* allows system administrators to define new DNS servers. The *Add DNS Server Page* page contains the following fields.

- **DNS Server IP Address** — Enter the DNS server's IP address.
- **Set DNS Server Active** — Defines active status of the new DNS Server. The possible values are:
  - *Checked*— This new server becomes the active DNS Server.
  - *Unchecked*— This new server is not the active DNS Server.

**STEP 3** Define the relevant fields.

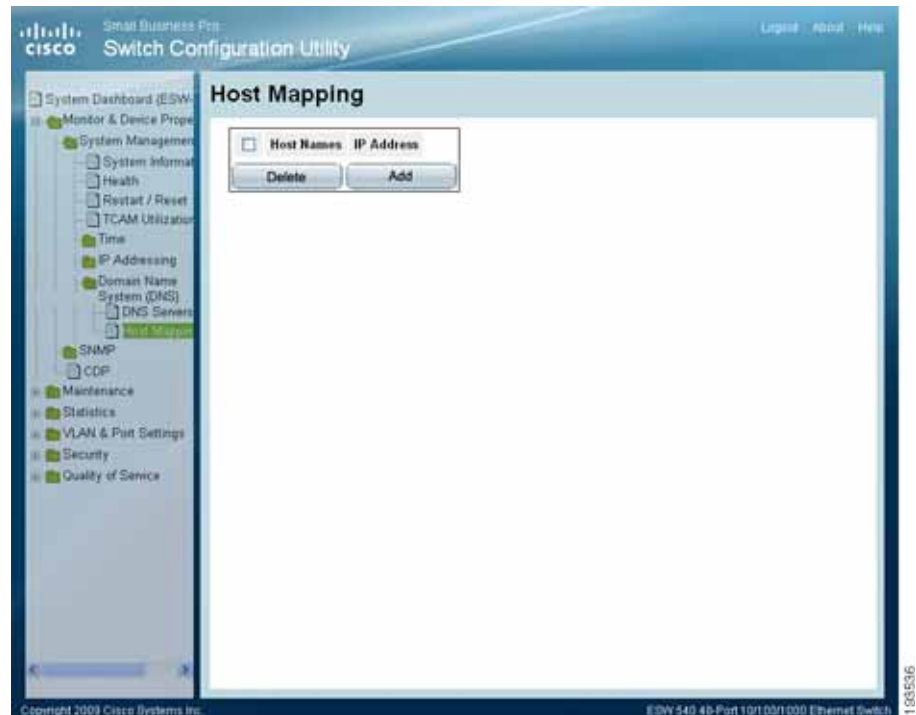
**STEP 4** Click **Apply**. The DNS server is added, and the device is updated.

### Mapping DNS Hosts

The *Host Mapping Page* provides information for defining DNS Host Mapping. To define the DNS Host Mapping:

- STEP 1** Click **Monitor & Device Properties > System Management > Domain Name System (DNS) > Host Mapping**. The *Host Mapping Page* opens:

#### Host Mapping Page



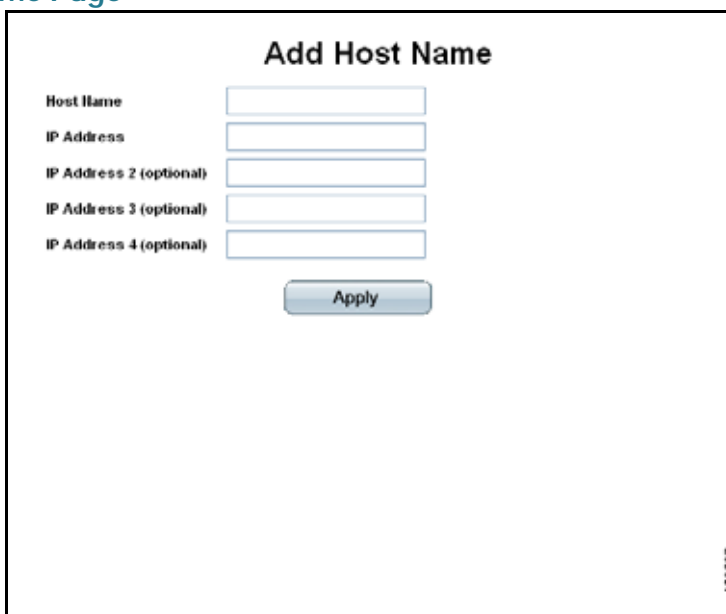
The *Host Mapping Page* contains the following fields:

- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.

- STEP 2** Click the **Add** button. The *Add Host Name Page* opens:

The *Add Host Name Page* provides information for defining DNS Host Mapping.

#### Add Host Name Page

The screenshot shows a web interface titled "Add Host Name". It contains five input fields arranged vertically, each with a label to its left: "Host Name", "IP Address", "IP Address 2 (optional)", "IP Address 3 (optional)", and "IP Address 4 (optional)". Below these fields is a blue "Apply" button. The entire form is enclosed in a black rectangular border. A small vertical text "1024537" is visible in the bottom right corner of the form area.

The *Add Host Name Page* contains the following fields:

- **Host Name** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The *Host Name* field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.
- **IP Address 2 (optional)** — Indicates the second network assigned to the interface. The address must be a valid address, specified in hexadecimal.
- **IP Address 3 (optional)** — Indicates the third network assigned to the interface. The address must be a valid address, specified in hexadecimal.
- **IP Address 4 (optional)** — Indicates the fourth network assigned to the interface. The address must be a valid address, specified in hexadecimal.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The DNS Host settings are defined, and the device is updated.

# Defining Address Tables

MAC addresses are stored in either the Static Address or the Dynamic Address databases. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frames source address. Frames addressed to a destination MAC address that is not associated with any port, are flooded to all ports of the relevant VLAN. Static addresses are manually configured. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased.

This section contains information for defining both static and dynamic Forwarding Database entries, and includes the following topics:

- Defining Static Addresses
- Defining Dynamic Addresses

## Defining Static Addresses

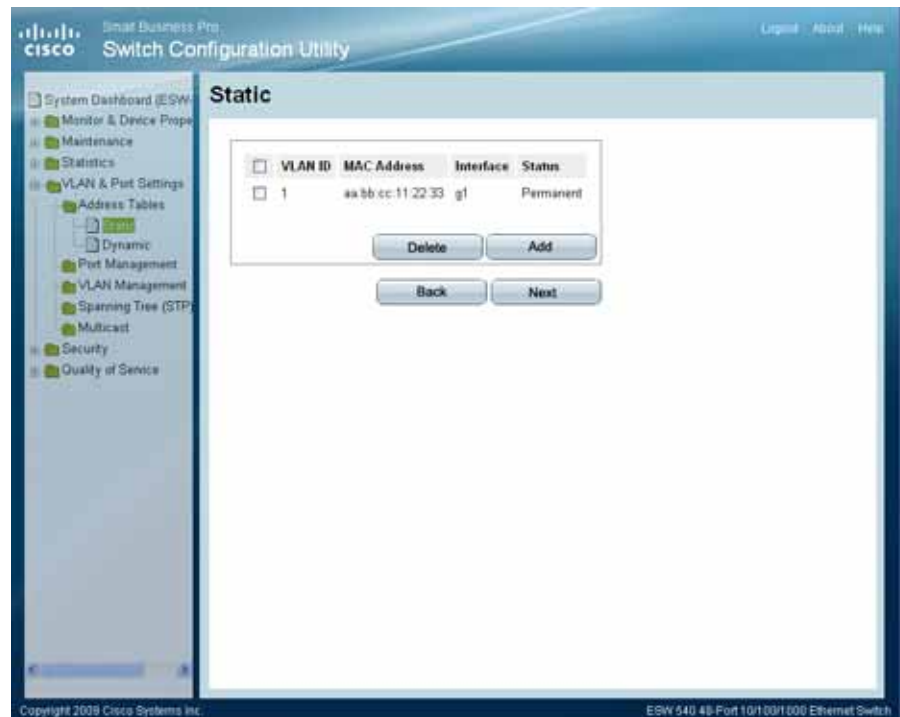
A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and cannot be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

To define static addresses:



**STEP 1** Click **VLAN & Port Settings > Address Tables > Static**. The *Static Page* opens:

#### Static Page



The *Static Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **MAC Address** — Displays the MAC address to which the entry refers.
- **Interface** — Displays the interface to which the entry refers:
  - *Port* — The specific port number to which the forwarding database parameters refer.
  - *EtherChannel* — The specific EtherChannel number to which the forwarding database parameters refer.
- **Status** — Displays how the entry was created. The possible field values are:
  - *Permanent* — The MAC address is permanent.
  - *Delete on Reset* — The MAC address is deleted when the device is reset.

## Defining Address Tables

### Defining Static Addresses

- *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
- *Secure* — The MAC Address is defined for locked ports.

**STEP 2** Click the **Add** button. The *Add Static MAC Address Page* opens:

#### Add Static MAC Address Page



The *Add Static MAC Address Page* contains the following fields:

- **Interface** — Defines the interface to which the entry refers:
  - *Port* — The specific port number to which the forwarding database parameters refer.
  - *EtherChannel* — The specific EtherChannel number to which the forwarding database parameters refer.
- **MAC Address** — Defines the MAC address to which the entry refers.
- **VLAN ID** — Defines the VLAN ID number to which the entry refers.
- **VLAN Name** — Defines the VLAN name to which the entry refers.
- **Status** — Defines how the entry is created. The possible field values are:
  - *Permanent* — The MAC address is permanent.
  - *Delete on Reset* — The MAC address is deleted when the device is reset.
  - *Delete on Timeout* — The MAC address is deleted when a timeout occurs.
  - *Secure* — The MAC Address is defined for locked ports.

## Defining Address Tables

### Defining Dynamic Addresses

---

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Static MAC Address is added, and the device is updated.

---

## Defining Dynamic Addresses

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

The *Dynamic Page* contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, and VLAN. The Dynamic MAC Address table contains information about the aging time before a dynamic MAC address is erased. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address.

## Defining Address Tables

### Defining Dynamic Addresses

- STEP 1** Click **VLAN & Port Settings > Address Tables > Dynamic**. The *Dynamic Page* opens:

#### Dynamic Page

Dynamic

Aging Interval: 300 (Sec)

Clear Table: ☐

Query by:

☐ Interface Port:  EtherChannel:

☐ MAC Address:

☐ VLAN ID:

Address Table Sort Key: VLAN

Query

VLAN ID	MAC	Interface
VLAN 1	0017a43aba70	g12
VLAN 1	001b8fa0422	g12
VLAN 1	001c251ced19	g7
VLAN 1	00211bf676ca	g12
VLAN 1	0021566501af	g7
VLAN 100	00000cd974d4	g12
VLAN 100	0021566501af	g7

Back Next

Apply

The *Dynamic Page* contains the following fields:

- **Aging Interval** — Specifies the amount of time in seconds the MAC address remains in the Dynamic MAC Address table before it is timed out, if no traffic from the source is detected. The default value is 300 seconds.
- **Clear Table** — If checked, clears the MAC address table.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. Dynamic addressing is defined, and the device is updated.

### Query By Section

In the Query By section, select the preferred option for sorting the addresses table:

- **Interface** — Specifies the interface for which the table is queried. The query can search for a specific port or EtherChannel.
- **MAC Address** — Specifies the MAC address for which the table is queried.
- **VLAN ID** — Specifies the VLAN ID for which the table is queried.
- **Address Table Sort Key** — Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.

**STEP 4** Define the relevant fields

**STEP 5** Click **Query**. The Dynamic MAC Address Table is queried, and the results are displayed.

---

# Configuring Multicast Forwarding

The Multicast section contains the following pages:

- IGMP Snooping
- Defining Multicast Group
- Defining Multicast Forwarding
- Defining Unregistered Multicast Settings

## IGMP Snooping

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

Configuring IGMP Snooping requires steps involving multiple pages of the switch configuration utility. Overall steps are:

- 
- STEP 1** Go to **VLAN & Port Settings->Multicast->IGMP Snooping**. Enabling IGMP Snooping Status.
  - STEP 2** Go to **VLAN & Port Settings->Multicast->Multicast Group**. Enabling Bridge Multicast Filtering.
  - STEP 3** Go to **VLAN & Port Settings->Multicast->Unregistered Multicast**. Update the applicable ports to Filtering.
-



**NOTE** In addition to the ESW500 switch configuration, PIM router (for example, the UC500) is configured in upstream router.

To enable IGMP Snooping:

- STEP 1** Click **VLAN & Port Settings > Multicast > IGMP Snooping**. The *IGMP Snooping Page* opens:

#### IGMP Snooping Page

VLAN ID	IGMP Snooping Status	Host Timeout	MRouter Timeout	Leave Timeout	
1	Disabled	260	300	10	Edit
2	Disabled	260	300	10	Edit

Apply

The *IGMP Snooping Page* contains the following fields:

- **Enable IGMP Snooping Status** — Indicates that the device monitors network traffic to determine which hosts want to receive multicast traffic. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
  - *Checked* — Enables IGMP Snooping on the device.
  - *Unchecked* — Disables IGMP Snooping on the device.
- **VLAN ID** — Specifies the VLAN ID.

- **IGMP Snooping Status** — Indicates if IGMP snooping is enabled on the specific VLAN. The possible field values are:
  - *Enabled* — IGMP Snooping is enabled on the VLAN.
  - *Disabled* — IGMP Snooping is not enabled on the VLAN.
- **Host Timeout** — Indicates the amount of the time the Host waits to receive a message before it times out. The default value is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an *Immediate Leave* value. The default timeout is 10 seconds.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The IGMP Snooping Parameters are updated, and the device is updated.

---

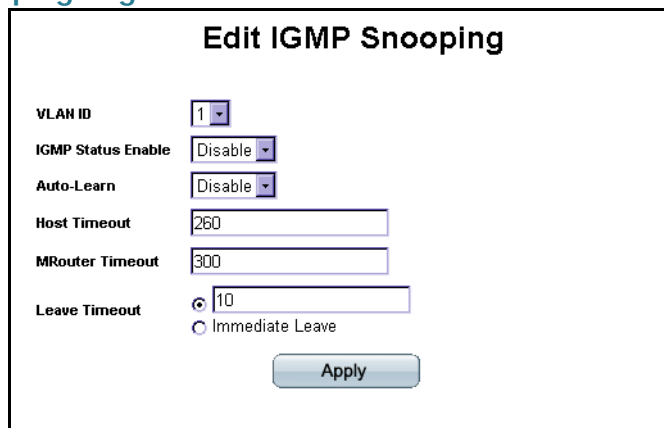
## Modifying IGMP Snooping

**STEP 1** Click **VLAN & Port Settings > Multicast > IGMP Snooping**. The *IGMP Snooping Page* opens:

**STEP 2** Click the **Edit** button. The *Edit IGMP Snooping Page*:



#### Edit IGMP Snooping Page



The screenshot shows the 'Edit IGMP Snooping' configuration page. It contains the following fields:

- VLAN ID**: A dropdown menu with '1' selected.
- IGMP Status Enable**: A dropdown menu with 'Disable' selected.
- Auto-Learn**: A dropdown menu with 'Disable' selected.
- Host Timeout**: A text input field with '260'.
- MRouter Timeout**: A text input field with '300'.
- Leave Timeout**: A radio button group with '10' selected (radio button) and 'Immediate Leave' (radio button).
- Apply**: A button at the bottom right.

The *Edit IGMP Snooping Page* contains the following fields:

- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Status Enable** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
  - *Enable* — Enables IGMP Snooping on the VLAN.
  - *Disable* — Disables IGMP Snooping on the VLAN.
- **Auto Learn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. The possible field values are:
  - *Enable* — Enables auto learn.
  - *Disable* — Disables auto learn.
- **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out. The default value is 300 seconds.
- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic. The Leave Timeout value is either user-defined, or an *Immediate Leave* value. The default timeout is 10 seconds.

#### STEP 3 Define the relevant fields.

## Configuring Multicast Forwarding

### Defining Multicast Group

- STEP 4** Click **Apply**. The IGMP Snooping Parameters are modified, and the device is updated.

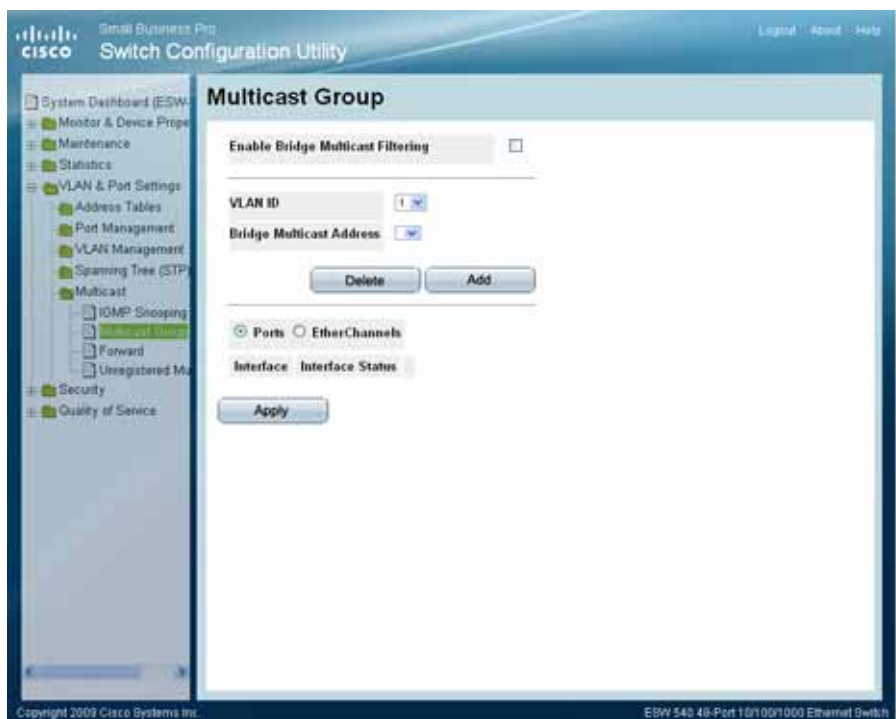
## Defining Multicast Group

The *Multicast Group Page* displays the ports and EtherChannels that are members of Multicast service groups. The Port and EtherChannel tables also reflect the manner in which the port or EtherChannels joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The *Multicast Group Page* permits new Multicast service groups to be created. The *Multicast Group Page* also assigns ports to a specific Multicast service address group.

To define Multicast group:

- STEP 1** Click **VLAN & Port Settings > Multicast > Multicast Group**. The *Multicast Group Page* opens:

### Multicast Group Page



The *Multicast Group Page* contains the following fields:

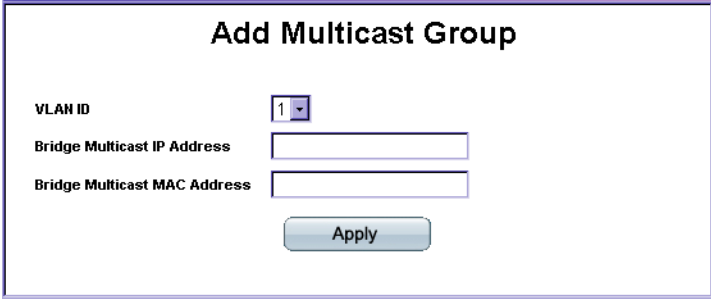
## Configuring Multicast Forwarding

### Defining Multicast Group

- **Enable Bridge Multicast Filtering** — Indicates if Bridge Multicast Filtering is enabled on the device. Bridge Multicast Filtering can be enabled only if IGMP Snooping is enabled. The possible field values are:
  - *Checked* — Enables Multicast Filtering on the device.
  - *Unchecked* — Disables Multicast Filtering on the device.
- **VLAN ID** — Specifies the VLAN ID.
- **Bridge Multicast Address** — Identifies the Multicast group MAC address.
- **Ports** — Displays the Multicast Group ports' status.
- **EtherChannels** — Displays the Multicast Group status of all of the device's EtherChannels.
- **Interface** — Displays the interface on which the Multicast service is configured.
- **Interface Status** — Displays the interface status. The options are as follows:
  - *Static* — Attaches the interface to the Multicast group as static member in the Static Row. The interface has joined the Multicast group statically in the Current Row.
  - *Forbidden* — Forbidden interfaces are not included the Multicast group, even if IGMP Snooping designated the interface to join a Multicast group.
  - *None* — The interface is not part of a Multicast group.

**STEP 2** Click the **Add** button. The *Add Multicast Group Page* opens:

#### Add Multicast Group Page



**Add Multicast Group**

VLAN ID

Bridge Multicast IP Address

Bridge Multicast MAC Address

The *Add Multicast Group Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.

## Configuring Multicast Forwarding

### Defining Multicast Group

- **Bridge Multicast IP Address** — Displays the IP address attached to the Multicast Group.
- **Bridge Multicast MAC Address** — Displays the MAC address attached to the Multicast Group.

**STEP 3** Define the relevant fields.

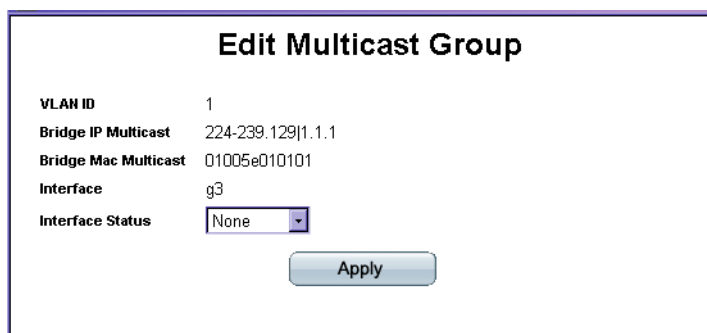
**STEP 4** Click **Apply**. The Multicast Group is added, and the device is updated.

## Modifying a Multicast Group

**STEP 1** Click **VLAN & Port Settings > Multicast > Multicast Group**. The *Multicast Group Page* opens:

**STEP 2** Click the **Edit** button. The *Edit Multicast Group Page* opens.

### Edit Multicast Group Page



The screenshot shows the 'Edit Multicast Group' configuration page. It contains the following fields and values:

Field	Value
VLAN ID	1
Bridge IP Multicast	224-239.129 1.1.1
Bridge Mac Multicast	01005e010101
Interface	g3
Interface Status	None

An 'Apply' button is located at the bottom right of the form.

The *Edit Multicast Group Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Bridge IP Multicast** — Displays the IP address attached to the Multicast Group.
- **Bridge MAC Multicast** — Displays the MAC address attached to the Multicast Group.
- **Interface** — Displays the interface attached to the Multicast Group.
- **Interface Status** — Defines the interface status. The options are as follows:

## Configuring Multicast Forwarding

### Defining Multicast Forwarding

---

- *Static* — Attaches the interface to the Multicast group as static member in the Static Row. The interface has joined the Multicast group statically in the Current Row.
- *Forbidden* — Forbidden interfaces are not included the Multicast group, even if IGMP Snooping designated the interface to join a Multicast group.
- *Excluded* — The port is not part of a Multicast group.
- *Dynamic* — The port received an IGMP Join report for this group - and is a dynamic member of the group. The multicast flow for this group will be forwarded to the port.

**STEP 3** Change the **Interface Status**.

**STEP 4** Click **Apply**. The Multicast Group parameters are modified, and the device is updated.

---

## Defining Multicast Forwarding

The *Multicast Forward Page* contains fields for attaching ports or EtherChannels to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN.

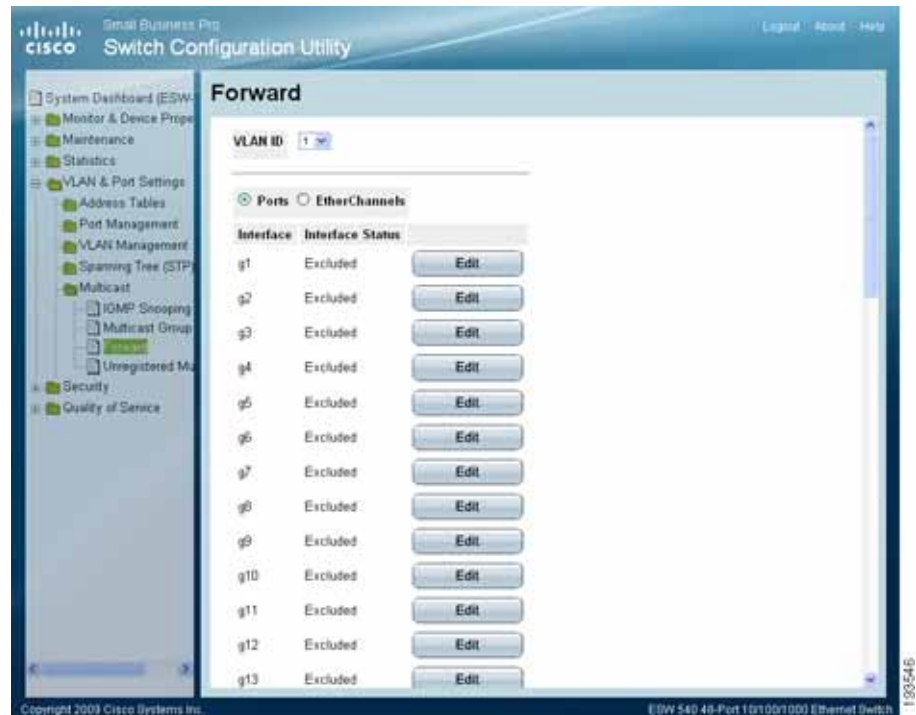
To define Multicast forward settings:

## Configuring Multicast Forwarding

### Defining Multicast Forwarding

- STEP 1** Click **VLAN & Port Settings > Multicast > Forward**. The *Multicast Forward Page* opens:

#### Multicast Forward Page



The *Multicast Forward Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Ports** — Displays the Multicast Forwarding ports' status.
- **EtherChannels** — Displays the Multicast Forwarding status of all of the device's EtherChannels.
- **Interface** — Indicates the port or EtherChannel whose Multicast forwarding configuration is described.
- **Interface Status** — Displays the interface status. The options are as follows:
  - *Static* — Attaches the port to the Multicast group as static member.
  - *Forbidden* — Forbidden ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
  - *Excluded* — The port is not part of a Multicast group.

## Configuring Multicast Forwarding

### Defining Multicast Forwarding

- *Dynamic* — Attaches the port to the Multicast group as dynamic member.

## Modifying Multicast Forwarding

**STEP 2** Click **VLAN & Port Settings > Multicast > Forward**. The *Multicast Forward Page* opens:

**STEP 3** Click the **Edit** button. The *Edit Multicast Forward All Page* opens:

### Edit Multicast Forward All Page



**Edit Multicast Forward All**

VLAN ID 1

Interface g1

Interface Status Static

Apply

The *Edit Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID.
- **Interface** — Displays the port or EtherChannel attached to the Multicast Group.
- **Interface Status** — Displays the interface status of the port or EtherChannel. The options are as follows:
  - *Static* — Attaches the interface to the Multicast group as a static member.
  - *Forbidden* — Forbidden interfaces are not included the Multicast group, even if IGMP snooping designated the interface to join a Multicast group.
  - *Excluded* — The interface is not part of a Multicast group.
  - *Dynamic* — Attaches the interface or EtherChannel dynamically to the Multicast group.

**STEP 4** Define the relevant fields.

---

**STEP 5** Click **Apply**. The Multicast Forward All settings are modified, and the device is updated.

---

## Defining Unregistered Multicast Settings

Multicast frames are generally forwarded to all ports in the VLAN. If IGMP Snooping is enabled, the device learns about the existence of Multicast groups and monitors which ports have joined what Multicast group. Multicast groups can also be statically enabled. This enables the device to forward the Multicast frames (from a registered Multicast group) only to ports that are registered to that Multicast group.

The *Unregistered Multicast Page* contains fields to handle Multicast frames that belong to Unregistered Multicast groups. Unregistered Multicast groups are the groups that are not known to the device. All Unregistered Multicast frames are still forwarded to all ports on the VLAN. After a port has been set to Forwarding/Filtering, then this port's configuration is valid for any VLAN it is a member of (or will be a member of).

To define unregistered Multicast settings:



## Configuring Multicast Forwarding

### Defining Unregistered Multicast Settings

- STEP 1** Click **VLAN & Port Settings > Multicast > Unregistered Multicast**. The *Unregistered Multicast Page* opens:

#### Unregistered Multicast Page



The Unregistered Multicast Page contains the following fields:

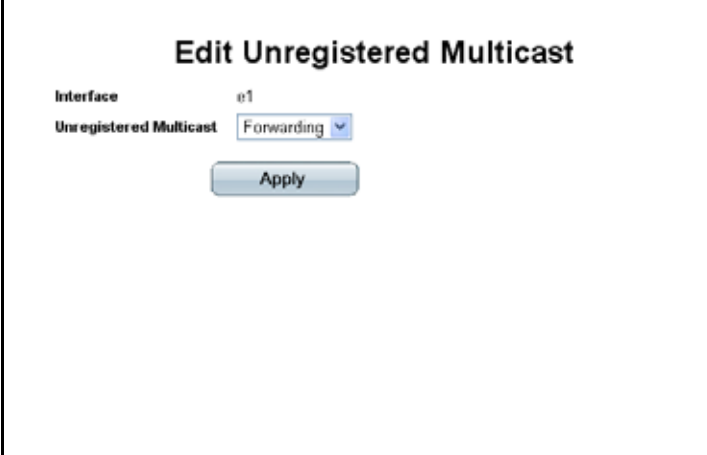
- **Ports** — Indicates the port for which the unregistered Multicast parameters are displayed.
- **EtherChannels** — Specifies the EtherChannel for which the Unregistered Multicast settings are displayed.
- **Interface** — Displays the interface ID.
- **Unregistered Multicast** — Indicates the forwarding status of the selected interface. The possible values are:
  - *Forwarding* — Enables forwarding of Unregistered Multicast frames to the selected VLAN interface. This is the default setting.
  - *Filtering* — Enables filtering of Unregistered Multicast frames to the selected VLAN interface.

- STEP 2** Click **Edit**. The Edit Unregistered Multicast Page opens:

## Configuring Multicast Forwarding

### Defining Unregistered Multicast Settings

#### Edit Unregistered Multicast Page



The screenshot displays a web-based configuration interface for a network device. The main heading is "Edit Unregistered Multicast". Below this, there are two configuration fields: "Interface" with the value "e1" and "Unregistered Multicast" with a dropdown menu currently showing "Forwarding". At the bottom of the configuration area is a blue "Apply" button. The entire configuration area is enclosed in a black rectangular border.

**STEP 3** Define the *Unregistered Multicast* field.

**STEP 4** Click **Apply**. The Multicast Forward All settings are saved and the device is updated.

# Configuring Spanning Tree

The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The device supports the following Spanning Tree versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops.
- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
- **Multiple STP** — Provides full connectivity for packets allocated to any VLAN. Multiple STP is based on the RSTP. In addition, Multiple STP transmits packets assigned to different VLANs through different MST regions. MST regions act as a single bridge.

The Spanning Tree section contains the following topics:

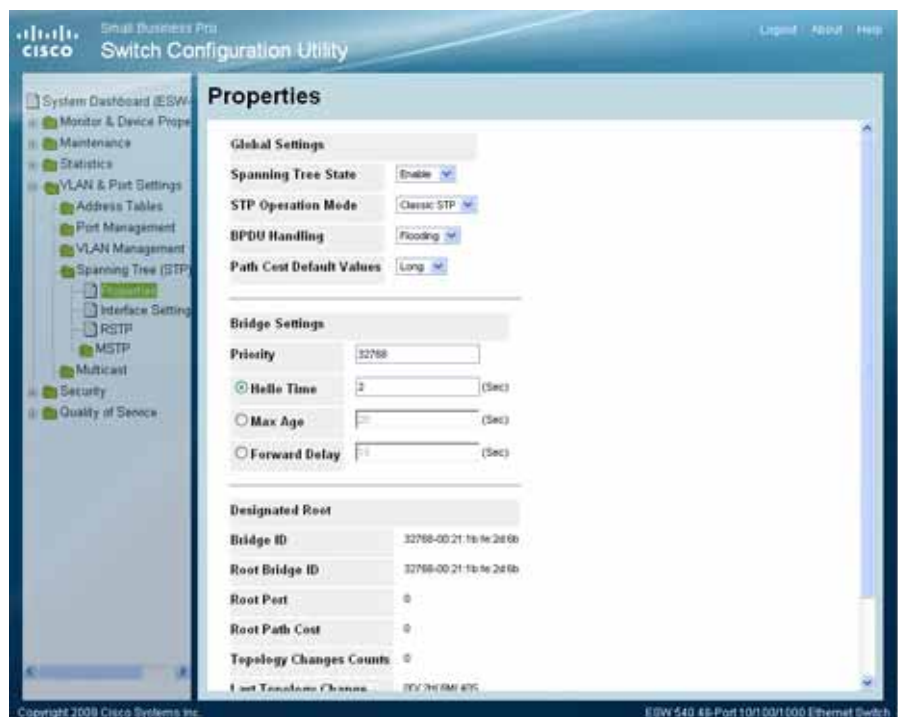
- Defining STP Properties
- Defining Spanning Tree Interface Settings
- Defining Rapid Spanning Tree
- Defining Multiple Spanning Tree

## Defining STP Properties

The *STP Properties Page* contains parameters for enabling STP on the device. The *STP Properties Page* is divided into three areas, Global Settings, Bridge Settings, and Designated Root.

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > Properties**. The *STP Properties Page* opens:

#### STP Properties Page



The *STP Properties Page* contains the following fields:

#### Global Settings

The Global Settings area contains device-level parameters.

- **Spanning Tree State** — Indicates if STP is enabled on the device. The possible field values are:
  - *Enable* — Enables STP on the device. This is the default value.
  - *Disable* — Disables STP on the device.
- **STP Operation Mode** — Indicates the STP mode that is enabled on the device. The possible field values are:
  - *Classic STP* — Enables Classic STP on the device. This is the default value.

- *Rapid STP* — Enables Rapid STP on the device.
  - *Multiple STP* — Enables Multiple STP on the device.
- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or device. BPDUs are used to transmit spanning tree information. The possible field values are:
  - *Filtering* — Filters BPDU packets when spanning tree is disabled on an interface.
  - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.
- **Path Cost Default Values** — Specifies the method used to assign default path costs to STP ports. The possible field values are:
  - *Short* — Specifies 1 through 65,535 range for port path costs.
  - *Long* — Specifies 1 through 200,000,000 range for port path costs. The default path costs assigned to an interface varies according to the selected method. This is the default value.

The Bridge Settings area contains the following fields:

- **Priority** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, etc. The range is 0 to 61440.
- **Hello Time** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The default is 2 seconds. The range is 1 to 10 seconds.
- **Max Age** — Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds that the device can wait without receiving a configuration message, before attempting to redefine its own configuration. The default max age is 20 seconds. The range is 6 to 40 seconds.
- **Forward Delay** — Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a learning state before forwarding packets. The default is 15 seconds. The range is 4 to 30 seconds.

The Designated Root area contains the following fields:

## Configuring Spanning Tree

### Defining Spanning Tree Interface Settings

---

- **Bridge ID** — Identifies the Bridge Priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root.
- **Root Path Cost** — The cost of the path from this bridge to the root.
- **Topology Changes Counts** — Indicates the total amount of STP state changes that have occurred.
- **Last Topology Change** — Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in a day hour minute second format, for example, 2 days 5 hours 10 minutes and 4 seconds.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. STP is enabled, and the device is updated.

---

## Defining Spanning Tree Interface Settings

Network administrators can assign STP settings to specific interfaces in the *STP Interface Settings Page*.

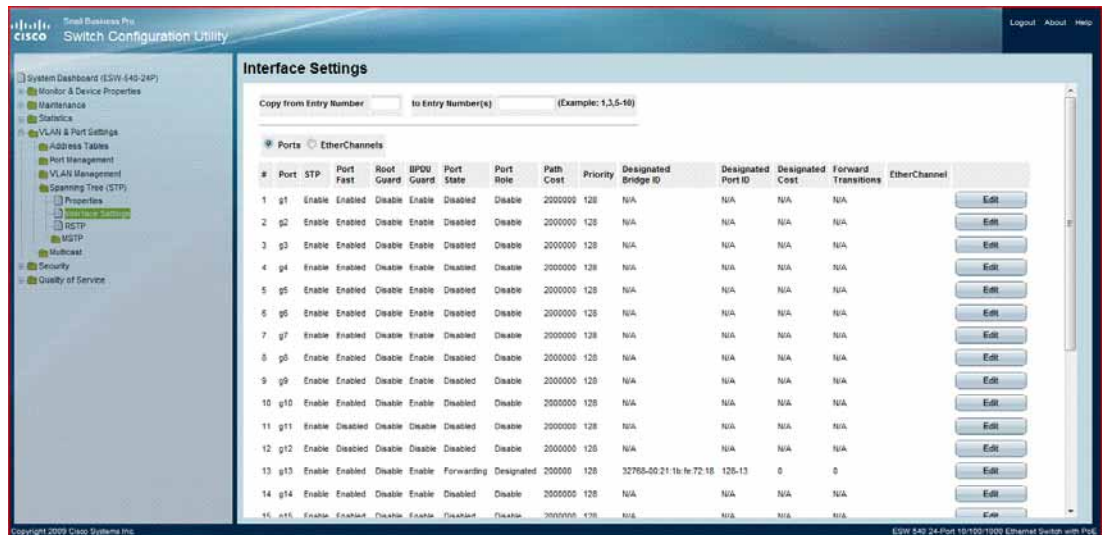
To assign STP settings to an interface:

## Configuring Spanning Tree

### Defining Spanning Tree Interface Settings

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > Interface Settings**. The *STP Interface Settings Page* opens:

#### Interface Settings Page



The *STP Interface Settings Page* contains the following fields:

- **Copy From Entry Number** — Indicate the port from which the STP interface setting are copied.
- **To Entry Number(s)** — Indicate the port to which the STP interface setting are copied.
- **Interface** — Displays the STP Interface settings of device ports.
- **Ports** — Display the STP Interface settings of device ports.
- **EtherChannels** — Display the STP Interface settings of device EtherChannels.
- **Port** — Indicates the port or EtherChannel on which STP is enabled.
- **STP** — Indicates if STP is enabled on the port. The possible field values are:
  - *Enable* — Indicates that STP is enabled on the port.
  - *Disables* — Indicates that STP is disabled on the port.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol

convergence. STP convergence can take 30-60 seconds in large networks. The possible values are:

- *Enabled* — Port Fast is enabled.
  - *Disable* — Port Fast is disabled.
  - *Auto* — Port Fast mode is enabled a few seconds after the interface becomes active.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root. Root Guard may be enabled or disabled.
- **BPDU Guard** — Indicates if BPDU Guard is enabled on the interface. BPDU Guard protects the network from invalid configurations. It is usually used either when fast link ports (ports connected to clients) are enabled or when STP is disabled. If a BPDU message is received, the port shuts down and the device generates an appropriate SNMP trap. The possible field values are:
  - *Enable* — Enables BPDU guard on the selected port or EtherChannel.
  - *Disable* — Disables BPDU guard on the selected port or EtherChannel. This is the default value.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
  - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Port Role** — Displays the port role assigned by the STP algorithm to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to the root switch.



## Configuring Spanning Tree

### Defining Spanning Tree Interface Settings

---

- *Designated* — The port or EtherChannel through which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.
  - *Disabled* — The port is not participating in the Spanning Tree.
- **Path Cost** — Indicates the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
  - **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority range is between 0-240. The priority value is provided in increments of 16.
  - **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
  - **Designated Port ID** — Indicates the selected port's priority and interface.
  - **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
  - **Forward Transitions** — Indicates the number of times the port has changed from the **Blocking** state to **Forwarding** state.
  - **EtherChannel** — Indicates the EtherChannel to which the port belongs. If a port is a member of a EtherChannel, the EtherChannel settings override the port settings.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. STP is enabled on the interface, and the device is updated.

---

## Modifying Interface Settings

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > Interface Settings**. The *Interface Settings Page* opens:
- STEP 2** Click the **Edit** button. The *Edit Interface Settings Page* opens:

### Edit Interface Settings Page

**Edit Interface Settings**

Interface: g1

STP: Enable

Port Fast: Enabled

Enable Root Guard: ☐

Enable BPDU Guard: ☒

Port State: Disabled

Speed: 1000M

Path Cost: 2000000

Default Path Cost: ☐

Priority: 128

Designated Bridge ID: N/A

Designated Port ID: N/A

Designated Cost: N/A

Forward Transitions: N/A

Ether Channel:

Apply

The *Edit Interface Settings Page* contains the following fields:

- **Interface** — Selects the port number on which Spanning Tree is configured.
- **STP** — Enables or disables STP on the port. The possible field values are:
  - *Enable* — Enables STP on the port.
  - *Disable* — Disables STP on the port.
- **Port Fast** — Indicates if Fast Link is enabled on the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks. The possible values are:

- *Enabled* — Enables Port Fast on the port.
  - *Disabled* — Disables Port Fast on the port.
  - *Auto* — Enables Port Fast mode a few seconds after the interface becomes active.
- **Enable Root Guard** — Enable the prevention of a devices outside the network core from being assigned the spanning tree root. The possible field values are:
  - *Checked* — Enables Root Guard on the selected port or EtherChannel.
  - *Unchecked* — Disables Root Guard on the selected port or EtherChannel. This is the default value.
- **Enable BPDU Guard** — Protects the network from invalid configurations. The possible field values are:
  - *Checked* — Enables BPDU Guard on the selected port or EtherChannel.
  - *Unchecked* — Disables BPDU Guard on the selected port or EtherChannel. This is the default value.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
  - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Speed** — Indicates the speed at which the port is operating.
- **Path Cost** — Defines the port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- **Default Path Cost** — Defines the default path cost as the Path Cost field setting. The possible field values are:

- *Checked* — Path Cost is the default value.
- *Unchecked* — Path Cost is user-defined.
- **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0 -240. The priority value is provided in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port's priority and interface.
- **Designated Cost** — Indicates the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — Indicates the number of times the port has changed from the **Blocking** state to **Forwarding** state.
- **EtherChannel** — Indicates the EtherChannel to which the port belongs. If a port is a member of a EtherChannel, the EtherChannel settings override the port settings.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The interface settings are modified, and the device is updated.

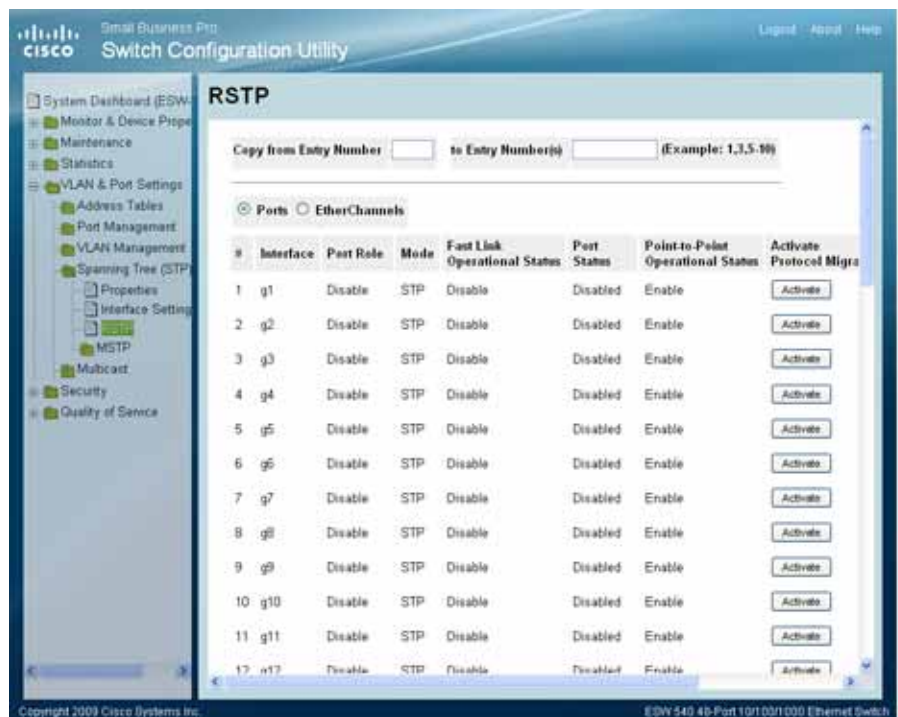
---

## Defining Rapid Spanning Tree

While the classic spanning tree prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops, and propagating status topology changes. Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops.

**STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > RSTP**. The *RSTP Page* opens:

#### RSTP Page



The *RSTP Page* contains the following fields:

- **Copy From Entry Number** — Indicate the port from which the STP interface setting are copied.
- **To Entry Number(s)** — Indicate the port to which the STP interface setting are copied.
- **Ports or EtherChannels Radio Buttons**— Indicates the port for which the STP settings are displayed.
- **Interface** — Indicates the Port or EtherChannels for which the STP settings are displayed.
- **EtherChannels** — Display the RSTP configurations of device EtherChannels.
- **Port Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to root switch.

- *Designated* — Indicates that the port or EtherChannel via which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - *Disable* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
  - *STP* — Indicates that Classic STP is enabled on the port.
  - *RSTP* — Indicates that Rapid STP is enabled on the port.
- **Fast Link Operational Status** — Indicates if Fast Link is enabled or disabled for the port or EtherChannel. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state. The possible field values are:
  - *Enable* — Fast Link is enabled.
  - *Disable* — Fast Link is disabled.
  - *Auto* — Fast Link mode is enabled a few seconds after the interface becomes active.
- **Port Status** — Indicates the RSTP status on the specific port. The possible field values are:
  - *Disabled* — Indicates that STP is currently disabled on the port.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
  - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.

## Configuring Spanning Tree

### Defining Rapid Spanning Tree

- **Point-to-Point Operational Status** — Indicates the Point-to-Point operating state. The possible values are:
  - Enable — Enables Point-to-Point on the interface.
  - Disable — Disables Point-to-Point on the interface.
- **Activate Protocol Migration** — Click the **Activate** button to run a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The Rapid Spanning Tree Settings are defined, and the device is updated.

## Modifying RTSP

**STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > RSTP**. The *RSTP Page* opens:

**STEP 2** Click the **Edit** button. The *Edit Rapid Spanning Tree Page* opens:

### Edit Rapid Spanning Tree Page



The screenshot shows the 'Edit Rapid Spanning Tree' configuration window. It contains the following fields and controls:

Field	Value/Control
Interface	Port g1 (selected), EtherChannel 1 (available)
Role	Disable
Mode	STP
Fast Link Operational Status	Disable
Port State	Disabled
Point to Point Admin Status	Auto (dropdown)
Point to Point Operational Status	Enable
Activate Protocol Migration Test	<input type="checkbox"/>

An 'Apply' button is located at the bottom center of the form.

The *Edit Rapid Spanning Tree Page* contains the following fields:

- **Interface** — Specifies whether Rapid STP is enabled is enabled on a port or EtherChannel.

- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to root switch.
  - *Designated* — Indicates that the port or EtherChannel via which the designated switch is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root switch from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - *Disable* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
  - *STP* — Indicates that Classic STP is enabled on the port.
  - *RSTP* — Indicates that Rapid STP is enabled on the port.
- **Fast Link Operational Status** — Indicates if Fast Link is enabled or disabled for the port or EtherChannel. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
  - *Enable* — Fast Link is enabled.
  - *Disable* — Fast Link is disabled.
  - *Auto* — Fast Link mode is enabled a few seconds after the interface becomes active.
- **Port State** — Indicates the RSTP status on the specific port. The possible field values are:
  - *Disabled* — Indicates that STP is currently disabled on the port.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
  - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.



- *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Point-to-Point Admin Status** — Indicates whether a point-to-point link is established on the port. Ports defined as Full Duplex are considered Point-to-Point port links. The possible field values are:
  - *Enable* — Device establishes point-to-point, full duplex links.
  - *Disable* — Device establishes shared, half duplex links.
  - *Auto* — Device automatically determines the state.
- **Point-to-Point Operational Status** — Indicates the Point-to-Point operating state.
- **Activate Protocol Migration Test** — Enables a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface. The possible field values are:
  - *Checked* — Enable Protocol Migration.
  - *Unchecked* — Disable Protocol Migration

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Rapid Spanning Tree Settings are modified, and the device is updated.

---

## Defining Multiple Spanning Tree

MSTP provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port is placed in the Forwarding State in another STP instance. The *MSTP Properties* page contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

The MSTP section contains the following pages:

- Defining MSTP Properties
- Defining MSTP Instance to VLAN
- Defining MSTP Instance Settings

- Defining MSTP Interface Settings

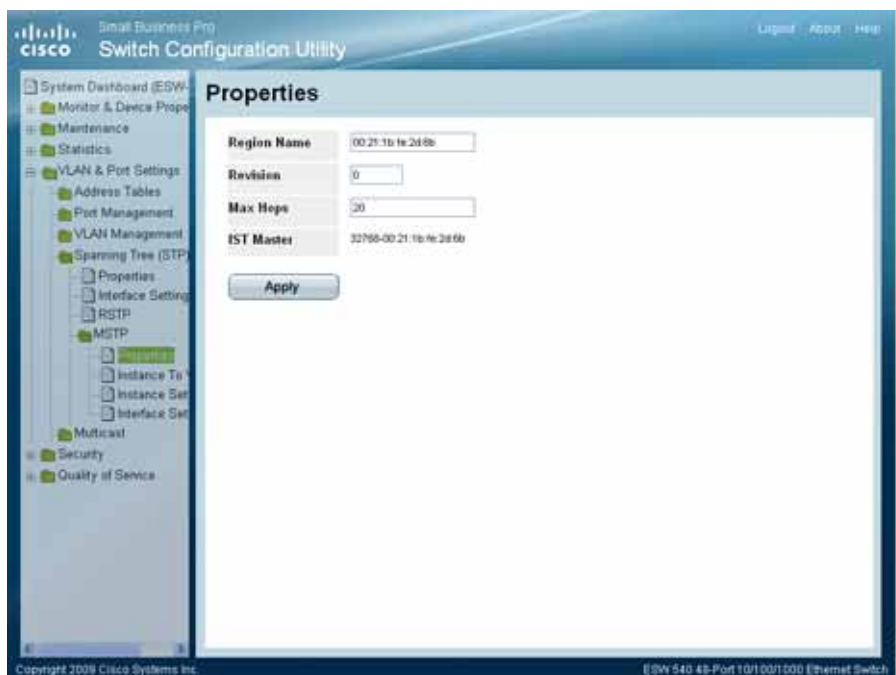
## Defining MSTP Properties

The *MSTP Properties Page* contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

To define MSTP:

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > MSTP > Properties**. The *MSTP Properties Page* opens:

### MSTP Properties Page



The *MSTP Properties Page* contains the following fields:

- **Region Name** — Provides a user-defined STP region name.
- **Revision** — Defines unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration. The possible field range 0-65535.
- **Max Hops** — Indicates the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port

## Configuring Spanning Tree

### Defining Multiple Spanning Tree

information is aged out. The possible field range is 1-40. The field default is 20 hops.

- **IST Master** — Identifies the region's master.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The MSTP properties are defined, and the device is updated.

---

## Defining MSTP Instance to VLAN

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

The VLAN page enables mapping VLANs to MSTP Instances.

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > MSTP > Instance to VLAN**. The *Instance to VLAN Page* opens:

#### Instance to VLAN Page

VLAN	Instance ID (0-15)	VLAN	Instance ID (0-15)	VLAN	Instance ID (0-15)	VLAN	Instance ID (0-15)
VLAN 1	0	VLAN 17	0	VLAN 33	0	VLAN 49	0
VLAN 2	0	VLAN 18	0	VLAN 34	0	VLAN 50	0
VLAN 3	0	VLAN 19	0	VLAN 35	0	VLAN 51	0
VLAN 4	0	VLAN 20	0	VLAN 36	0	VLAN 52	0
VLAN 5	0	VLAN 21	0	VLAN 37	0	VLAN 53	0
VLAN 6	0	VLAN 22	0	VLAN 38	0	VLAN 54	0
VLAN 7	0	VLAN 23	0	VLAN 39	0	VLAN 55	0
VLAN 8	0	VLAN 24	0	VLAN 40	0	VLAN 56	0
VLAN 9	0	VLAN 25	0	VLAN 41	0	VLAN 57	0
VLAN 10	0	VLAN 26	0	VLAN 42	0	VLAN 58	0
VLAN 11	0	VLAN 27	0	VLAN 43	0	VLAN 59	0
VLAN 12	0	VLAN 28	0	VLAN 44	0	VLAN 60	0
VLAN 13	0	VLAN 29	0	VLAN 45	0	VLAN 61	0
VLAN 14	0	VLAN 30	0	VLAN 46	0	VLAN 62	0
VLAN 15	0	VLAN 31	0	VLAN 47	0	VLAN 63	0
VLAN 16	0	VLAN 32	0	VLAN 48	0	VLAN 64	0

The *Instance to VLAN Page* contains the following fields:

- **VLAN** — Indicates the VLAN for which the MSTP instance ID is defined.
- **Instance ID (0-15)** — Indicates the MSTP instance ID assigned to the VLAN. The possible field range is 0-15.

- STEP 2** Map the VLANs to Instance IDs.

- STEP 3** Click **Apply**. The MSTP VLAN mapping is defined, and the device is updated.

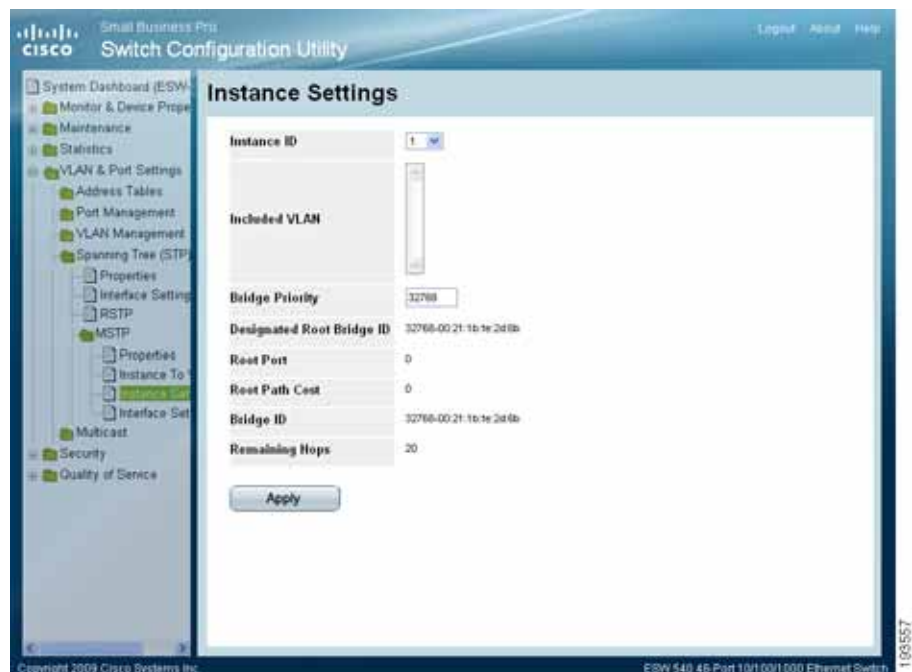
## Defining MSTP Instance Settings

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within *Multiple Spanning Tree Regions* (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

Network Administrators can define MSTP Instances settings using the *MSTP Instance Settings Page*.

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > MSTP > Instance Settings**. The *MSTP Instance Settings Page* opens:

### MSTP Instance Settings Page



The *MSTP Instance Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device.
- **Included VLAN** — Maps the selected VLAN to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The field range is 0-61440.

## Configuring Spanning Tree

### Defining Multiple Spanning Tree

---

- **Designated Root Bridge ID** — Indicates the priority and MAC address of the bridge with the lowest path cost to the instance ID.
- **Root Port** — Indicates the selected instance's root port.
- **Root Path Cost** — Indicates the selected instance's path cost.
- **Bridge ID** — Indicates the priority and MAC address of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The MSTP Instance configuration is defined, and the device is updated.

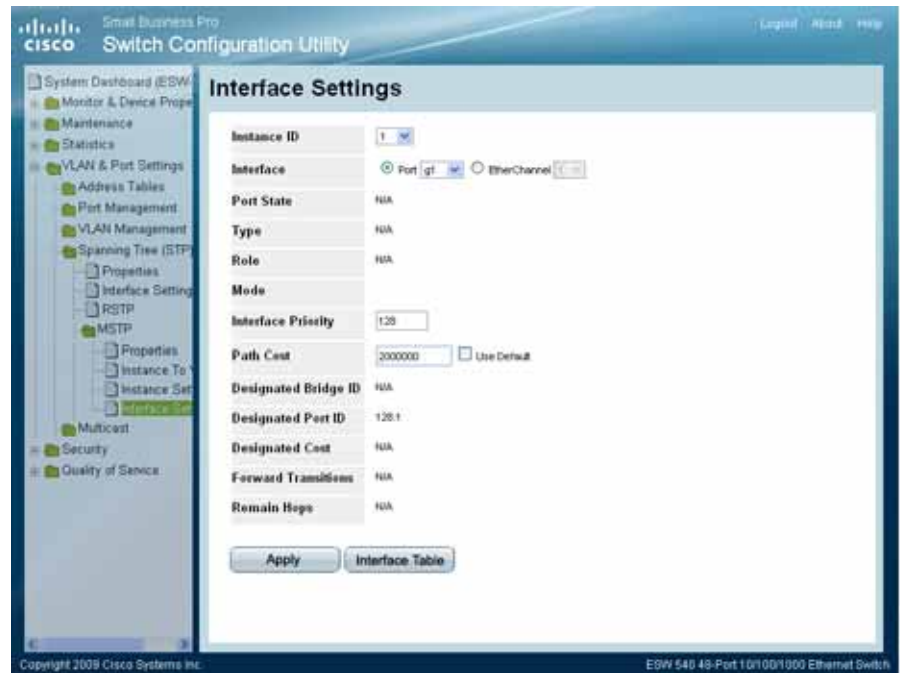
---

## Defining MSTP Interface Settings

Network Administrators can define MSTP Instances settings using the *MSTP Interface Settings Page*.

- STEP 1** Click **VLAN & Port Settings > Spanning Tree (STP) > MSTP > Interface Settings**. The *MSTP Interface Settings Page* opens:

#### MSTP Interface Settings Page



The *MSTP Interface Settings Page* contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 1-15.
- **Interface** — Displays the interface for which the MSTP settings are displayed. The possible field values are:
  - *Port* — Specifies the port for which the MSTP settings are displayed.
  - *EtherChannel* — Specifies the EtherChannel for which the MSTP settings are displayed.
- **Port State** — Indicates the MSTP status on the specific port. The possible field values are:
  - *Disabled* — Indicates that STP is currently disabled on the port.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.

- *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
  - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Type** — Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:
  - *Boundary Port* — Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode
  - *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
  - *Internal* — Indicates the port is an internal port.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to root device.
  - *Designated* — Indicates the port or EtherChannel via which the designated device is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root device from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
  - *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
  - *STP* — Indicates that Classic STP is enabled on the port.
  - *RTSP* — Indicates that Rapid STP is enabled on the port.
  - *MSTP* — Indicates that MSTP is enabled on the port.



## Configuring Spanning Tree

### Defining Multiple Spanning Tree

- **Interface Priority** — Defines the interface priority for specified instance. The priority value is between 0 -240. The priority value is provided in increments of 16. The default value is 128.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range is 1-200,000,000.
- **Designated Bridge ID** — Indicates the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Forward Transitions** — Indicates the number of times the port has changed from Forwarding state to Blocking state.
- **Remain Hops** — Indicates the hops remaining to the next destination.



#### TIP

The **Apply** button can be used to make changes to a single interface (Port or EtherChannel) instead of using the **Interface Table** button to make changes to multiple Ports or EtherChannels.

**STEP 2** Click the **Interface Table** button. The *MSTP Interface Table Page* opens:

## MSTP Interface Table Page

Interface Table										
Instance <span>1</span> Interface <input checked="" type="radio"/> Ports <input type="radio"/> EtherChannels										
Interface	Role	Mode	Type	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Role
g1	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g2	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g3	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g4	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g5	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g6	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g7	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g8	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g9	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g10	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g11	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g12	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g13	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
g14	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A

The *MSTP Interface Table Page* contains the following fields:

- **Instance** — Defines the VLAN group to which the interface is assigned.
- **Interface** — Indicates the port or EtherChannel for which the MSTP settings are displayed.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
  - *Root* — Provides the lowest cost path to forward packets to root device.
  - *Designated* — Indicates the port or EtherChannel via which the designated device is attached to the LAN.
  - *Alternate* — Provides an alternate path to the root device from the root interface.
  - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur

when a LAN has two or more connections connected to a shared segment.

- *Disabled* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
  - *STP* — Indicates that Classic STP is enabled on the device.
  - *RSTP* — Indicates that Rapid STP is enabled on the device.
  - *MSTP* — Indicates that MSTP is enabled on the port.
- **Type** — Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:
  - *Boundary Port* — Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode
  - *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
  - *Internal* — Indicates the port is an internal port.
- **Port Priority** — Defines the interface priority for specified instance. The default value is 128. The priority value is between 0 -240. The priority value is provided in increments of 16.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **Port State** — Indicates the MSTP status on the specific port. The possible field values are:
  - *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
  - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
  - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.

## Configuring Spanning Tree

### Defining Multiple Spanning Tree

---

- *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Designated Bridge ID** — Indicates the bridge ID number that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates the Port ID number on the designated bridge that connects the link or the shared LAN to the root.
- **Remain Hops** — Indicates the hops remaining to the next destination.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The MSTP Interface configuration is defined, and the device is updated.

---

# Configuring Quality of Service

Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

- Classifying incoming traffic into handling classes, based on an attribute, including:
  - The ingress interface
  - Packet content
  - A combination of these attributes
- Providing various mechanisms for determining the allocation of network resources to different handling classes, including:
  - The assignment of network traffic to a particular hardware queue
  - The assignment of internal resources
  - Traffic shaping

The terms Class of Service (CoS) and QoS are used in the following context:

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.
- QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

The QoS facility involves the following elements:

- **Access Control Lists (ACLs)** — Used to decide which traffic is allowed to enter the system, and which is to be dropped. Only traffic that meets this criteria are subject to CoS or QoS settings. ACLs are used in QoS and network security.

- **Traffic Classification** — Classifies each incoming packet as belonging to a given traffic class, based on the packet contents and/or the context.
- **Assignment to Hardware Queues** — Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong, as defined by the classification mechanism.
- **Traffic Class-Handling Attributes** — Applies QoS/CoS mechanisms to different classes, including: Bandwidth Management

The Quality of Service section contains the following topics:

- Managing QoS Statistics
- Defining General Settings
- Defining Advanced QoS Mode

## Managing QoS Statistics

The QoS Statistics section contains the following pages:

- Policer Statistics
- Aggregated Policer Statistics
- Queues Statistics

### Policer Statistics

The *Policer Statistics Page* indicates the amount of in-profile and out-of-profile packets that are received on an interface.

To add policer statistics:

- STEP 1** Click **Quality of Service > QoS Statistics > Policer Statistics**. The *Policer Statistics Page* opens:

#### Policer Statistics Page

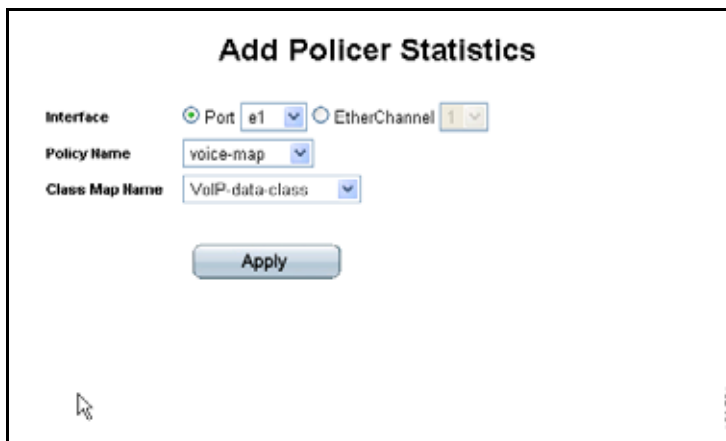


The *Policer Statistics Page* contains the following fields:

- **Interface** — Displays the interface (port or EtherChannel) for which Policer statistics are displayed.
- **Policy** — Displays the policy for which the statistics are displayed.
- **Class Map** — Displays the class map for which the statistics are displayed.
- **In-Profile Bytes** — Displays the total number in-profile bytes received on the interface.
- **Out-of-Profile Bytes** — Displays the total number out-profile bytes received on the interface.
- **Clear Counters** — Clicking this button will open a pop-up window that informs you "This will clear all statistics counters, would you like to proceed?"

You have the option of clicking **OK** to continue or **Cancel** to go back.

- STEP 2** Click the **Add** button. The *Add Policer Statistics Page* opens.



The *Add Policer Statistics Page* contains the following fields:

- **Interface** — Select either the Port or EtherChannel radio button to select the interface.
- **Policy Name** — Select the policy Name from the pull-down list.
- **Class Map Name** — Select the Class Map Name from the pull-down list.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Policer Statistics is defined, and the device is updated.

## Add Aggregated Policer Statistics

The *Aggregated Policer Statistics Page* indicates the amount of in-profile and out-of-profile packets that are received per aggregate policer name.

To add Aggregated Policer Statistics:



- STEP 1** Click **Quality of Service > QoS Statistics > Aggregate Policer**. The *Aggregate Policer Page* opens:


#### Aggregate Policer Page



The *Aggregate Policer Page* contains the following fields:

- **Aggregate Policer Name** — Indicates the port or EtherChannel on which the packets were received.
- **In-profile Bytes** — Displays the total number of in-profile packets that were received.
- **Out-of-profile Bytes** — Displays the total number of out-of-profile packets that were received.

**STEP 2** Click the **Add** button. The *Add Aggregate Policer Page* opens.



The Add Aggregate Policer Page includes one field: the Aggregate Policer Name.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Aggregate Police defined, and the device is updated.

## Resetting Aggregate Policer Statistics Counters

- STEP 1** Click **Quality of Service > QoS Statistics > Aggregate Policer**. The *Aggregate Policer Statistics Page* opens:



- STEP 2** Click **Clear Counters**. The Aggregate Policer statistics counters are cleared.

## Queues Statistics

The Queues Statistics Page contains parameters for viewing queue statistics including statistics forwarded and dropped packets based on interface, queue, and drop precedence.

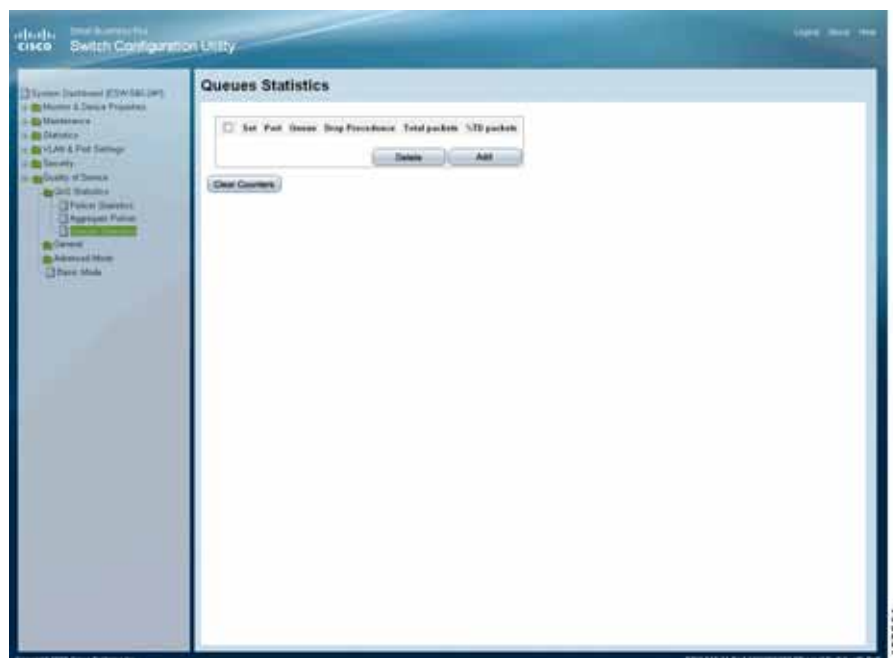


- NOTE** The Queues Statistics Page is applicable to Gigabit devices only, and will not appear in all switches.

To view the Queues Statistics page:

- STEP 1** Click **Quality of Service > QoS Statistics > Queues Statistics**. The *Queues Statistics Page* opens:

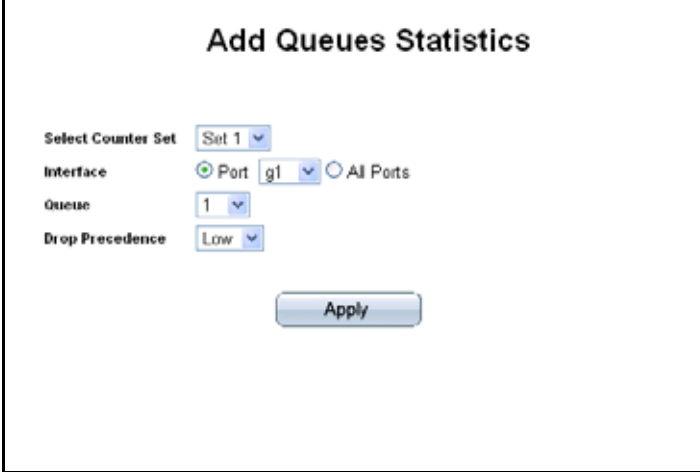
#### Queues Statistics Page



The Queues Statistics Page contains the following fields:

- **Set** — Displays the counter set. The possible field values are:
  - **1** — Displays the statistics for Set 1. Set 1 contains all interfaces and all queues with a high DP.
  - **2** — Displays the statistics for Set 2. Set 2 contains all interfaces and all queues with a low DP.
- **Port** — Displays the port for which the queue statistics are displayed.
- **Queue** — Displays the queue from which packets were forwarded or tail dropped.
- **Drop Precedence** — Displays the drop precedence assigned to the packets forwarded or tail dropped for which statistics are displayed.
- **Total packets** — Displays the total number of packets forwarded or tail dropped.
- **% TD packets** — Displays the percentage of packets that were tail dropped.

**STEP 2** Click the **Add** button. The *Add Queues Statistics Page* opens.



The screenshot shows a web form titled "Add Queues Statistics". It contains four configuration fields: "Select Counter Set" with a dropdown menu showing "Set 1"; "Interface" with radio buttons for "Port" (selected) and "All Ports", and a dropdown for "g1" next to "Port"; "Queue" with a dropdown menu showing "1"; and "Drop Precedence" with a dropdown menu showing "Low". An "Apply" button is located at the bottom center of the form.

### Adding Queues Statistics

- The *Add Queues Statistics* Page contains the following fields:
- **Select Counter Set** — Selects the counter set.
- **Interface** — Defines the ports for which statistics are displayed. The possible field values are:
  - **Port** — Selects the port or which statistics are displayed.
  - **All Ports** — Specifies that statistics are displayed for all ports.
- **Queue** — Selects the queue for which statistics are displayed.
- **Drop Precedence** — Selects the drop precedence assigned to the packets forwarded or tail dropped for which statistics are displayed.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Queues Statistics are defined, and the device is updated.

### Resetting Queue Statistics Counters

To clear the statistics counters, click the **Clear Counters** button.

## Defining General Settings

The QoS General Settings section contains the following pages:

- Defining CoS
- Defining QoS Queue
- Mapping CoS to Queue
- Mapping DSCP to Queue
- Configuring Bandwidth
- VLAN Rate Limit

### Defining CoS

The *CoS Page* contains fields for enabling or disabling CoS (Basic or Advanced mode). In addition, the default CoS for each port or EtherChannel is definable.

**STEP 1** Click **Quality of Service > General > CoS**. The *CoS Page* opens:

#### CoS Page



The *CoS Page* contains the following fields:

- **QoS Mode** — Indicates if QoS is enabled on the device. The possible values are:
  - *Advanced* — Enables Advanced mode QoS on the device.
  - *Basic* — Enables QoS on the device.
  - *Disable* — Disables QoS on the device.
- **Ports** — Indicates that the CoS configuration of the ports are described in the page.
- **EtherChannels** — Indicates that the CoS configuration of the EtherChannels are described in the page.
- **Interface** — Indicates the interface for which the CoS information is displayed.
- **Default CoS** — Displays the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.

## Configuring Quality of Service

### Defining General Settings

- **Restore Defaults** — Restores the factory CoS default settings to the selected port.
  - *Checked* — Restores the factory QoS default settings to ports after clicking the **Apply** button.
  - *Unchecked* — Maintains the current QoS settings.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The QoS Mode is defined, and the device is updated.

---

### Modifying Interface Priorities

**STEP 1** Click **Quality of Service > General > CoS**. The *CoS Page* opens:

**STEP 2** Click the **Edit** button. The *Edit Interface Priority Page* opens:

#### Edit Interface Priority Page



The screenshot shows the 'Edit Interface Priority' configuration page. At the top, there is a title 'Edit Interface Priority'. Below the title, there is a section labeled 'Interface' with two radio buttons: 'Port' (selected) and 'EtherChannel'. The 'Port' radio button is followed by a dropdown menu showing 'g1'. The 'EtherChannel' radio button is followed by a dropdown menu showing '1'. Below this section, there is a label 'Set Default User Priority' followed by a dropdown menu showing '0'. At the bottom of the page, there is a large blue 'Apply' button. The page has a light gray background and a white border.

The *Edit Interface Priority Page* contains the following fields:

- **Interface** — Indicates whether the interface is a port or EtherChannel.
- **Set Default User Priority** — Defines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.

**STEP 3** Modify the Interface priority.

**STEP 4** Click **Apply**. The Interface priority is set, and the device is updated.



## Defining QoS Queue

The *Queue Page* contains fields for defining the QoS queue forwarding types.

## Configuring Quality of Service

### Defining General Settings

**STEP 1** Click **Quality of Service > General > Queue**. The *Queue Page* opens:

#### Queue Page (non-Gigabit devices)

The screenshot shows the Cisco Small Business Pro Switch Configuration Utility interface. The left sidebar contains a tree view with the following items: System Dashboard (ESW), Monitor & Device Properties, Maintenance, Statistics, VLAN & Port Settings, Security, Quality of Service, QoS Statistics, General, CoS, Queue, CoS to Queue, DSCP to Queue, Bandwidth, VLAN Rate Limit, Advanced Mode, and Basic Mode. The 'Queue' item is selected. The main content area is titled 'Queue' and has a sub-header 'Fast Ethernet'. Below this, there are two radio buttons: 'Strict Priority' (unselected) and 'WRR' (selected). A table titled 'Scheduling' shows the following data:

Queue	WRR Weight	% of WRR Bandwidth
1	1	6.67
2	2	13.33
3	4	26.67
4	8	53.33

Below the table is a section for 'Giga Ethernet' with a similar 'Scheduling' table. This table has four columns: 'Queue', 'Strict Priority', 'WRR', 'WRR Weight', and '% of WRR Bandwidth'. The 'Strict Priority' column has radio buttons, and the 'WRR' column has radio buttons. The 'WRR Weight' column has input fields. The '% of WRR Bandwidth' column shows calculated values. The 'Apply' button is at the bottom of the 'Giga Ethernet' section.

Queue	Strict Priority	WRR	WRR Weight	% of WRR Bandwidth
1	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="1"/>	6.67
2	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="2"/>	13.33
3	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="4"/>	26.67
4	<input type="radio"/>	<input checked="" type="radio"/>	<input type="text" value="8"/>	53.33

Copyright 2008 Cisco Systems Inc. ESW 520 48-Port 10/100 Ethernet Switch with PoE 10-3568

#### Queue Page (Gigabit devices)

The screenshot shows the Cisco Switch Configuration Utility interface. On the left is a navigation tree with categories like System Dashboard, Monitor & Device Properties, Maintenance, Statistics, VLAN & Port Settings, Security, Quality of Service, and QoS Statistics. Under QoS Statistics, the 'Queue' option is selected. The main area is titled 'Queue' and contains a table for configuring queues. The table has columns for Queue, Strict Priority, WRR, WRR Weight, and % of WRR Bandwidth. Queue 1 has Strict Priority selected and WRR Weight of 10. Queue 2 has WRR selected and WRR Weight of 10. Queue 3 has WRR selected and WRR Weight of 35. Queue 4 has WRR selected and WRR Weight of 45. An 'Apply' button is at the bottom of the table.

Queue	Strict Priority	WRR	WRR Weight	% of WRR Bandwidth
1	<input checked="" type="radio"/>	<input type="radio"/>	10	10
2	<input type="radio"/>	<input checked="" type="radio"/>	10	10
3	<input type="radio"/>	<input checked="" type="radio"/>	35	35
4	<input type="radio"/>	<input checked="" type="radio"/>	45	45

Apply

The *Queue Page* contains the following fields:

- **Fast Ethernet** — Select whether traffic scheduling on Fast Ethernet interfaces is based on either Strict Priority or WRR. This field is applicable to FE devices only (not applicable to ESW 520-8P devices). The possible field values are:
  - *Strict Priority* — Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
  - *WRR* — Indicates that traffic scheduling for the selected queue is based strictly on the WRR. If WRR is selected, the predetermined weights 1, 2, 4 and 8 are assigned to queues 1, 2, 3 and 4 respectively.
- **Queue** — Displays the queue for which the queue settings are displayed. The possible field range is 1 - 4.
- **WRR Weight** — Displays the WRR weight assigned to the queue by the user.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the queue. These values represent the % of the WRR Weight configured by the user.

- **Giga Ethernet** — Enables configuring traffic scheduling on GE interfaces. This field heading is applicable to FE devices only.

The fields below are applicable to both FE and GE devices.

- **Queue** — Displays the queue for which the queue settings are displayed for GE interfaces. The possible field range is 1 - 4.
- **Strict Priority** — Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
- **WRR** — Indicates that traffic scheduling for the selected queue is based strictly on the WRR. If WRR is selected on FE Devices, the default WRR Weight of 1, 2, 4 and 8 are assigned to queues 1, 2, 3 and 4 respectively. If WRR is selected on GE Devices, the default WRR Weight of 10, 10, 35 and 45 are assigned to queues 1, 2, 3 and 4 respectively.
- **WRR Weight** — Displays the WRR weight assigned to the queue by the user.
- **% of WRR Bandwidth** — Indicates the amount of bandwidth assigned to the queue. These values represent the % of the WRR Weight configured by the user.

**STEP 2** Define the queues.

**STEP 3** Click **Apply**. The queues are defined, and the device is updated.

---

## Mapping CoS to Queue

The *Cos to Queue Page* contains fields for classifying CoS settings to traffic queues.

## Configuring Quality of Service

### Defining General Settings

**STEP 1** Click **Quality of Service > General > CoS to Queue**. The *Cos to Queue Page* opens:

#### Cos to Queue Page



The *Cos to Queue Page* contains the following fields:

- **Restore Defaults** — Restores all queues to the default CoS settings. The possible field values are:
  - Checked — Restores all queues to the default CoS settings.
  - Unchecked — Maintain the CoS settings currently defined.
- **Class of Service** — Specifies the CoS VLAN (CoS) priority tag values, where zero is the lowest and 7 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported, where Queue 4 is the highest and Queue 1 is the lowest.

**STEP 2** Define the relevant mapping.

**STEP 3** Click **Apply**. CoS to queues are mapped, and the device is updated.

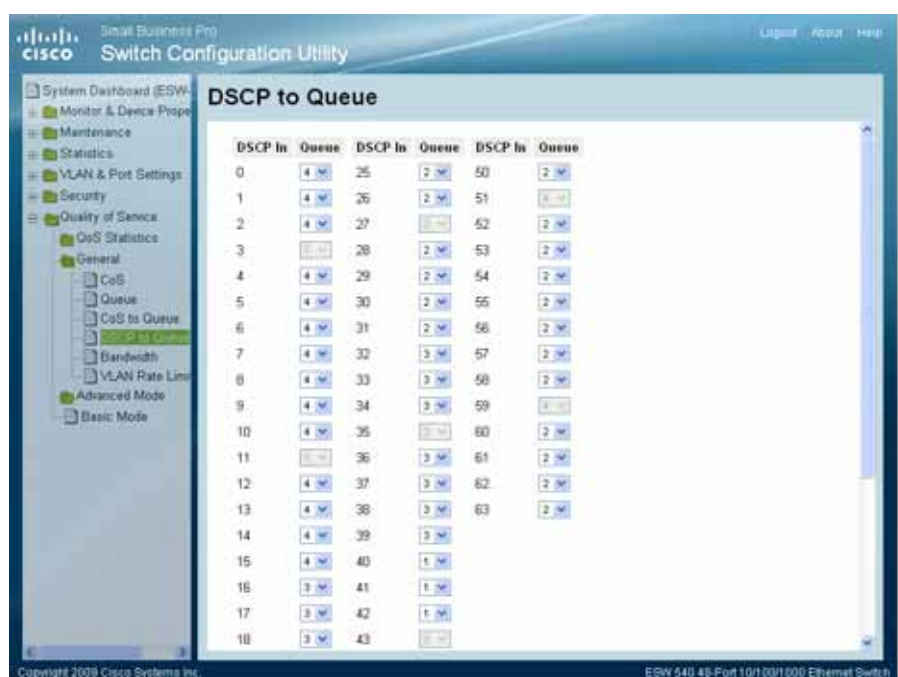
## Mapping DSCP to Queue

The *DSCP to Queue Page* enables mapping DSCP values to specific queues.

To map DSCP to Queues:

- STEP 1** Click **Quality of Service > General > DSCP to Queue**. The *DSCP to Queue Page* opens:

### DSCP to Queue Page



The *DSCP to Queue Page* contains the following fields:

- **DSCP In** — Indicates the Differentiated Services Code Point (DSCP) value in the incoming packet. The following values are reserved and cannot be changed: **3, 11, 19, 27, 35, 43, 51, and 59**.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped.

- STEP 2** Define the relevant mapping.

- STEP 3** Click **Apply**. DSCP to queues are mapped, and the device is updated.

## Configuring Bandwidth

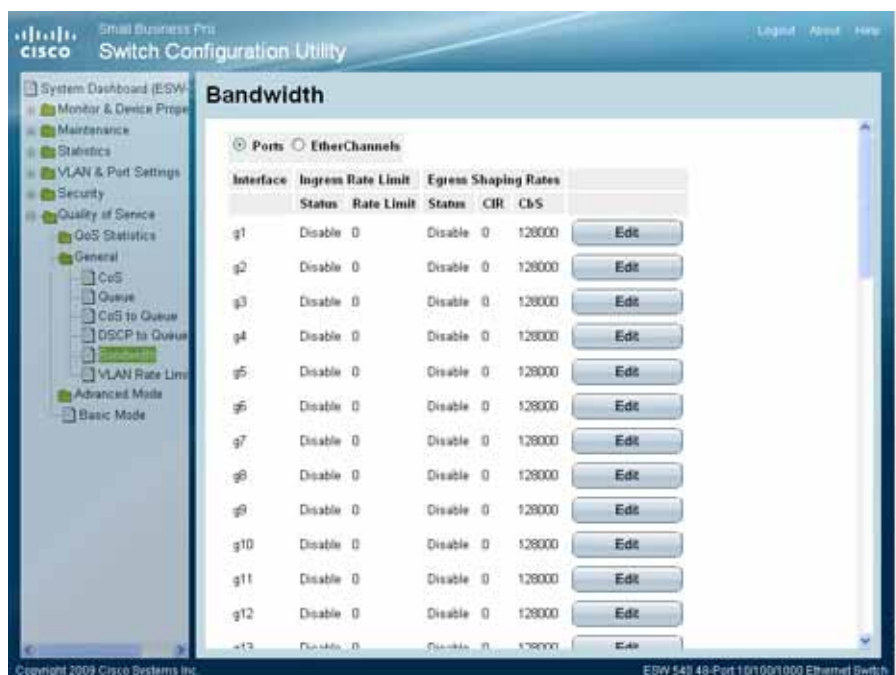
The *Bandwidth Page* allows network managers to define the bandwidth settings for specified egress and ingress interfaces.

Rate Limits and Shaping are defined per interface:

- Rate Limit sets the maximum bandwidth allowed on ingress interfaces.
- Shaping Rate sets the maximum bandwidth allowed on egress interfaces. On GE ports, traffic shape for burst traffic (CbS) can also be defined.

**STEP 1** Click **Quality of Service > General > Bandwidth**. The *Bandwidth Page* opens:

### Bandwidth Page



The *Bandwidth Page* contains the following fields:

- **Ports** — Indicates that the bandwidth settings of the ports are described in the page.
- **EtherChannels** — Indicates that the bandwidth settings of the EtherChannels are described in the page.
- **Interface** — Displays the interface (port or EtherChannel) for which the Bandwidth settings are made.

- **Ingress Rate Limit** — Indicates the traffic limit for ingress interfaces. The possible field values are:
  - *Status* — Enables or disables rate limiting for ingress interfaces. *Disable* is the default value.
  - *Rate Limit* — Defines the rate limit for ingress ports. Defines the amount of bandwidth assigned to the interface.  
For FE ports, the rate is 62 - 100,000 Kbps.  
For GE ports, the rate is 62 - 1,000,000 Kbps.
- **Egress Shaping Rates** — Indicates the traffic shaping type, if enabled, for egress ports. The possible field values are:
  - *CIR* — Defines Committed Information Rate (CIR) as the queue shaping type. The possible field values are:  
For FE ports, the rate is 64 - 62,500 Kbps.  
For GE ports, the rate is 64 - 1,000,000 Kbps.
  - *CbS* — Defines Committed Burst Size (CbS) as the queue shaping type. CbS is supported only on GE interfaces. The possible field value is 4096 - 16,769,020 bytes.
  - *Status* — Enables or disables rate limiting for egress interfaces. *Disable* is the default value.

## Modifying Bandwidth Settings

**STEP 2** Click **Quality of Service > General > Bandwidth**. The *Bandwidth Page* opens:

**STEP 3** Click the **Edit** button. The *Edit Bandwidth Page* opens:



#### Edit Bandwidth Page

**Edit Bandwidth**

Interface ☒ Port g1 ☐ EtherChannel 1

Enable Egress Shaping Rate ☐

Committed Information Rate (CIR)

Committed Burst Size (CBS)

Enable Ingress Rate Limit ☐

Ingress Rate Limit

Apply

The *Edit Bandwidth Page* contains the following fields:

- **Interface** — Indicates whether the interface, for which bandwidth settings are edited, is a port or a EtherChannel.
- **Enable Egress Shaping Rate** — Indicates if shaping is enabled on the interface. The possible field values are:
  - *Checked* — Enables egress shaping on the interface.
  - *Unchecked* — Disables egress shaping on the interface.
- **Committed Information Rate (CIR)** — Defines CIR as the queue shaping type. The possible field values are:
  - For FE ports, the rate is 64 - 62,500 Kbps.
  - For GE ports, the rate is 64 - 1,000,000 Kbps.
- **Committed Burst Size (CbS)** — Defines CbS as the queue shaping type. CbS is supported only on GE interfaces. The possible field value is 4096 - 16,769,020 bytes.
- **Enable Ingress Rate Limit** — Indicates if rate limiting is defined on the interface. The possible field values are:
  - *Checked* — Enables ingress rate limiting on the interface.
  - *Unchecked* — Disables ingress rate limiting on the interface.
- **Ingress Rate Limit** — Defines the amount of bandwidth assigned to the interface.

## Configuring Quality of Service

### Defining General Settings

For FE ports, the rate is 62 - 100,000 Kbps.  
For GE ports, the rate is 62 - 1,000,000 Kbps.

**STEP 4** Modify the relevant fields.

**STEP 5** Click **Apply**. The bandwidth settings are modified, and the device is updated.

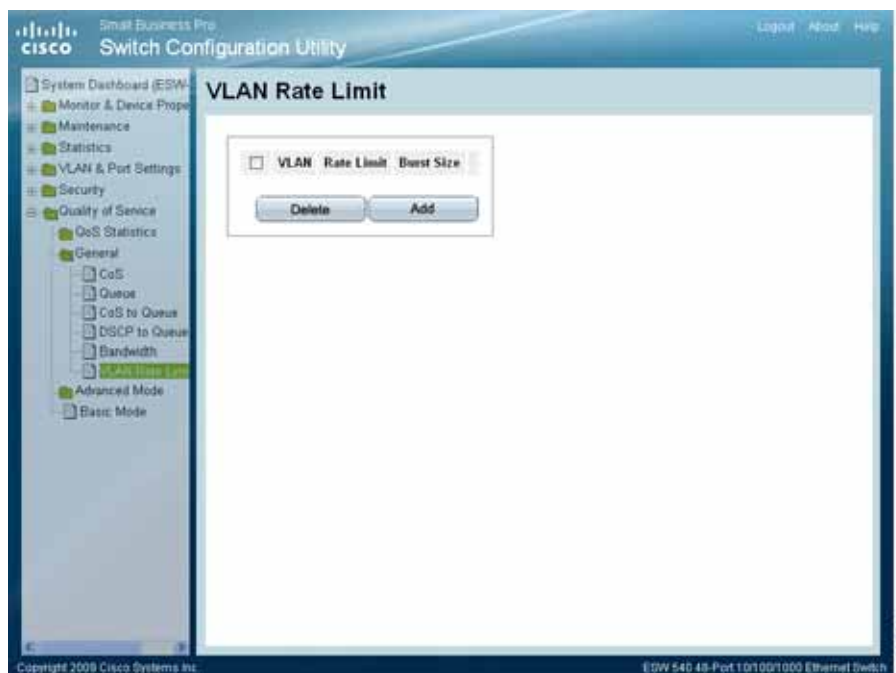
## Configuring VLAN Rate Limit

Rate limiting per VLAN allows network administrators to limit traffic on VLANs. Rate limiting is calculated separately for each packet processor in a unit. QoS rate limiting has priority over VLAN rate limiting. For example, if a packet is subject to QoS rate limits but is also subject to VLAN rate limiting, and the rate limits conflict, the QoS rate limits take precedence.

To define the VLAN Rate Limit:

**STEP 1** Click **Quality of Service > General > VLAN Rate Limit**. The *VLAN Rate Limit Page* opens:

### VLAN Rate Limit Page

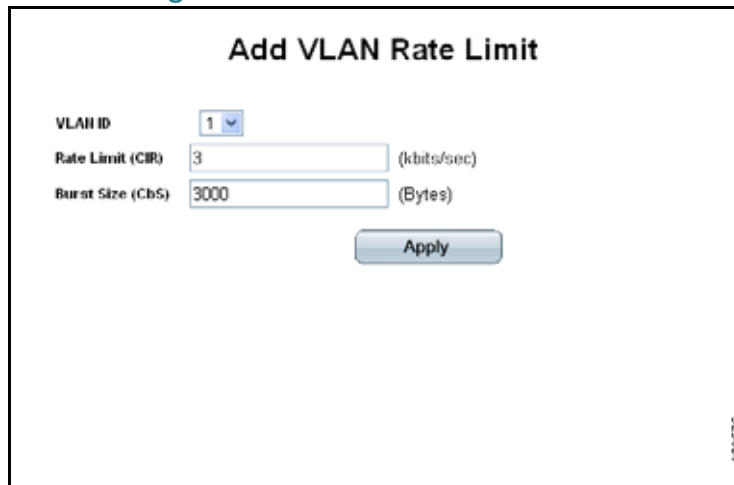


The *VLAN Rate Limit Page* contains the following fields:

- **VLAN** – Indicates the VLAN on which the Rate Limit is applied.
- **Rate Limit** – Defines the maximum rate (CIR) in kbits per second (bps) that forwarding traffic is permitted in the VLAN.
- **Burst Size** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

**STEP 2** Click the **Add** button. The *Add VLAN Rate Limit Page* opens:

#### Add VLAN Rate Limit Page



The *Add VLAN Rate Limit Page* contains the following fields.

- **VLAN ID** – Defines the VLAN on which to apply the Rate Limit.
- **Rate Limit (CIR)** – Defines the maximum rate (CIR) in Kbits per second (Kbps) that forwarding traffic is permitted in the VLAN.
- **Burst Size (CbS)** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

**STEP 3** Define the relevant fields.

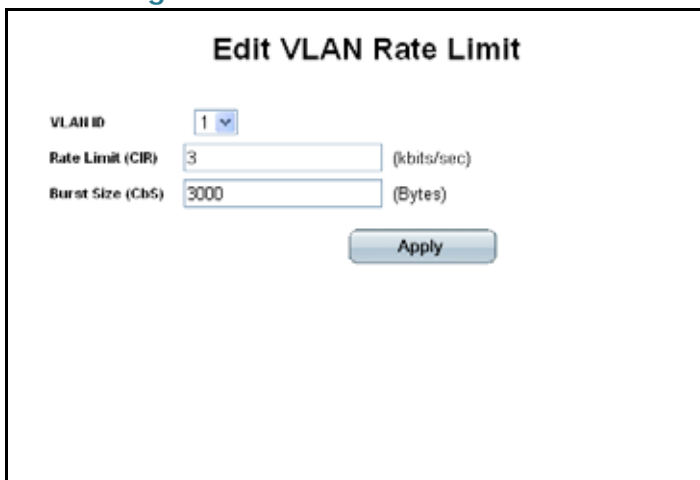
**STEP 4** Click **Apply**. The VLAN Rate Limit is added, and the device is updated.

## Modifying the VLAN Rate Limit

**STEP 1** Click **Quality of Service > General > VLAN Rate Limit**. The *VLAN Rate Limit Page* opens:

**STEP 2** Click the **Edit** button. The *VLAN Rate Limit Page* opens:

### Edit VLAN Rate Limit Page



The screenshot shows a web interface titled "Edit VLAN Rate Limit". It has three input fields: "VLAN ID" with a dropdown menu showing "1", "Rate Limit (CIR)" with a text box containing "3" and "(kbits/sec)" to its right, and "Burst Size (CbS)" with a text box containing "3000" and "(Bytes)" to its right. Below these fields is an "Apply" button.

The *VLAN Rate Limit Page* contains the following fields:

- **VLAN ID** – Defines the VLAN on which to apply the Rate Limit.
- **Rate Limit (CIR)** – Defines the maximum rate (CIR) in kbits per second (Kbps) that forwarding traffic is permitted in the VLAN.
- **Burst Size (CbS)** – Defines the maximum burst size (CbS) in bytes that forwarding traffic is permitted through the VLAN.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The VLAN Rate Limit is modified, and the device is updated.

## Defining Advanced QoS Mode

Advanced QoS mode provides rules for specifying flow classification and assigning rule actions that relate to bandwidth management. The rules are defined in classification control lists (CCL).

CCLs are set according to the classification defined in the ACL, and they cannot be defined until a valid ACL is defined. When CCLs are defined, ACLs and CCLs can be grouped together in a more complex structure, called policies. Policies can be applied to an interface. Policy ACLs/CCLs are applied in the sequence they appear within the policy. Only a single policy can be attached to a port.

In advanced QoS mode, ACLs can be applied directly to an interface. However, a policy and ACL cannot be simultaneously applied to an interface.

After assigning packets to a specific queue, services such as configuring output queues for the scheduling scheme, or configuring output shaping for burst size, CIR, or CbS per interface or per queue, can be applied.

The *Advanced Mode* section contains the following topics:

- Configuring DSCP Mapping
- Defining Class Mapping
- Defining Aggregate Policer
- Configuring Policy Table
- Defining Policy Binding

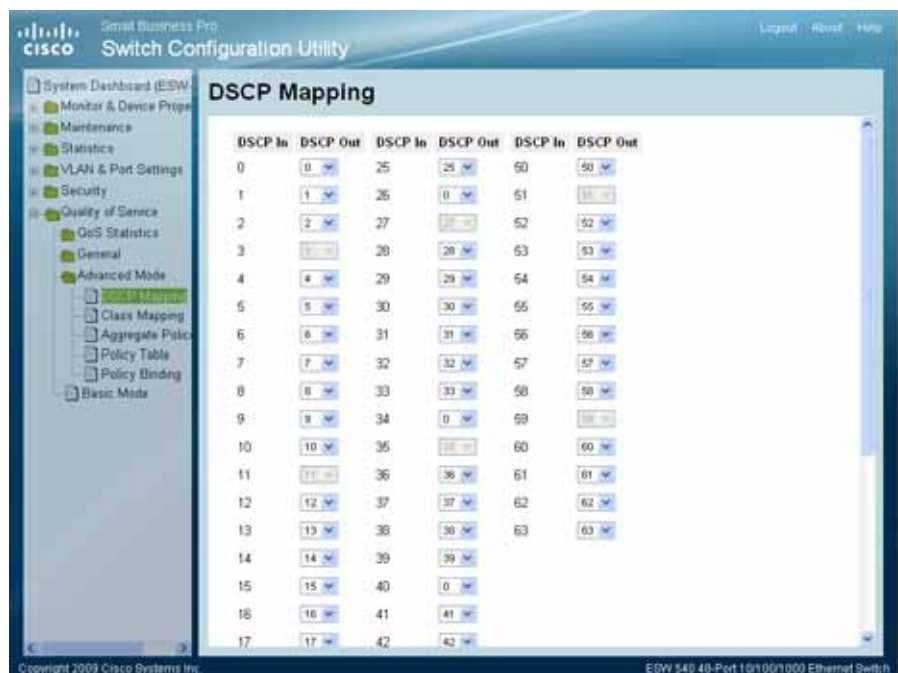
## Configuring DSCP Mapping

The *DSCP Mapping Page* enables mapping Differentiated Services Code Point (DSCP) values from incoming packets to DSCP values in outgoing packets. The DSCP values can be modified only within the queue range. This information is important when traffic exceeds user-defined limits.

To map DSCP values:

- STEP 1** Click **Quality of Service > Advanced Mode > DSCP Mapping**. The *DSCP Mapping Page* opens:

#### DSCP Mapping Page



The *DSCP Mapping Page* contains the following fields:

- **DSCP In** — Indicates the DSCP value in the incoming packet which will be mapped to an outgoing packet.
- **DSCP Out** — Sets a mapped DSCP value in the outgoing packet for the corresponding incoming packet.

- STEP 2** Define the relevant mapping.

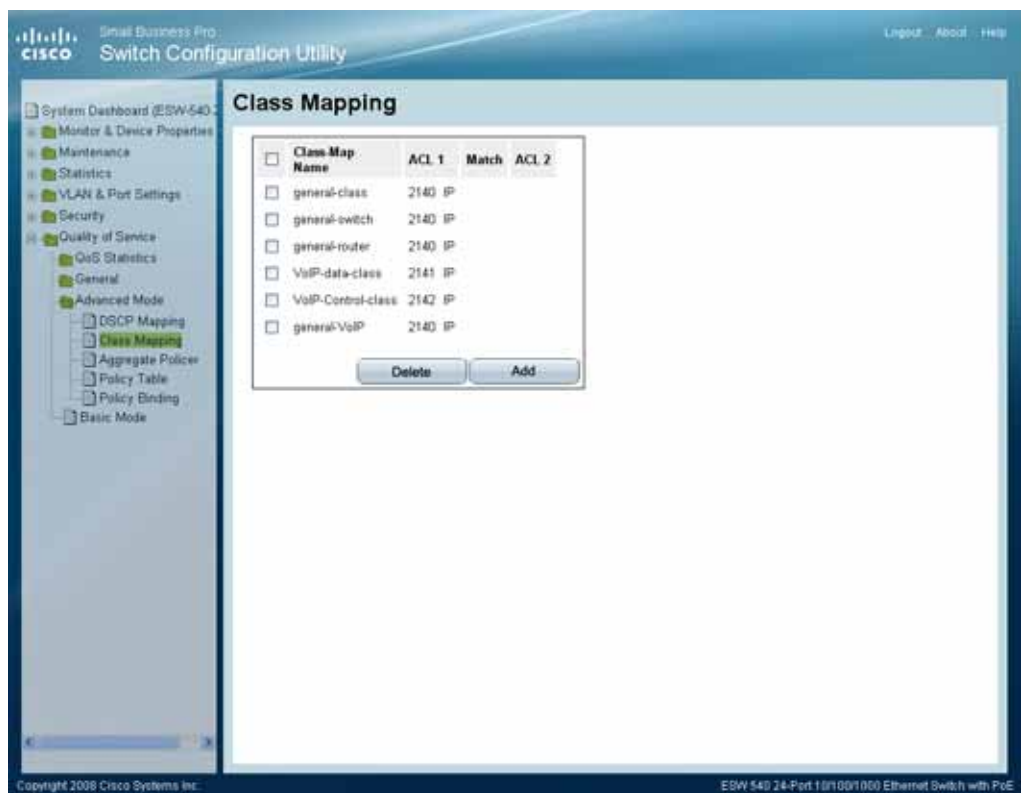
- STEP 3** Click **Apply**. DSCP incoming values are mapped to DSCP outgoing values, and the device is updated.

## Defining Class Mapping

The *Class Mapping Page* contains parameters for defining class maps. One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned to packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL.

**STEP 1** Click **Quality of Service > Advanced Mode > Class Mapping**. The *Class Mapping Page* opens:

### Class Mapping Page



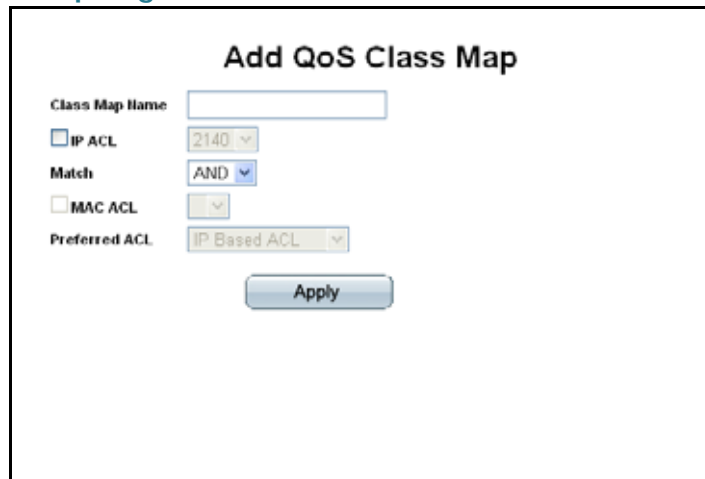
The *Class Mapping Page* contains the following fields:

- **Class Map Name** — Selects an existing Class Map by name.
- **ACL 1** — Contains a list of the user-defined ACLs.
- **Match** — Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:

- *AND*— Both the ACL 1 and the IP-based ACL 2 must match a packet.
- *OR*— Either the ACL 1 or the ACL 2 must match a packet.
- **ACL 2** — Contains a list of the user-defined ACLs.

**STEP 2** Click the **Add** button. The *Add QoS Class Map Page* opens:

#### Add QoS Class Map Page



The *Add QoS Class Map Page* contains the following fields.

- **Class Map Name** — Defines a new Class Map name
- **IP ACL** — Matches packets to IP based ACLs first, then matches packets to MAC based ACLs.
- **Match** — Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:
  - *AND*— Both the MAC-based and the IP-based ACL must match a packet.
  - *OR* — Either the MAC-based or the IP-based ACL must match a packet.
- **MAC ACL** — Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.
- **Preferred ACL** — Defines if packets are first matched to an IP based ACL or a MAC based ACL. The possible field values are:
  - *IP Based ACLs*— Matches packets to IP based ACLs first, then matches packets to MAC based ACLs.



- *MAC Based ACLs* — Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. QoS mapping is added, and the device is updated.

---

## Defining Aggregate Policer

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

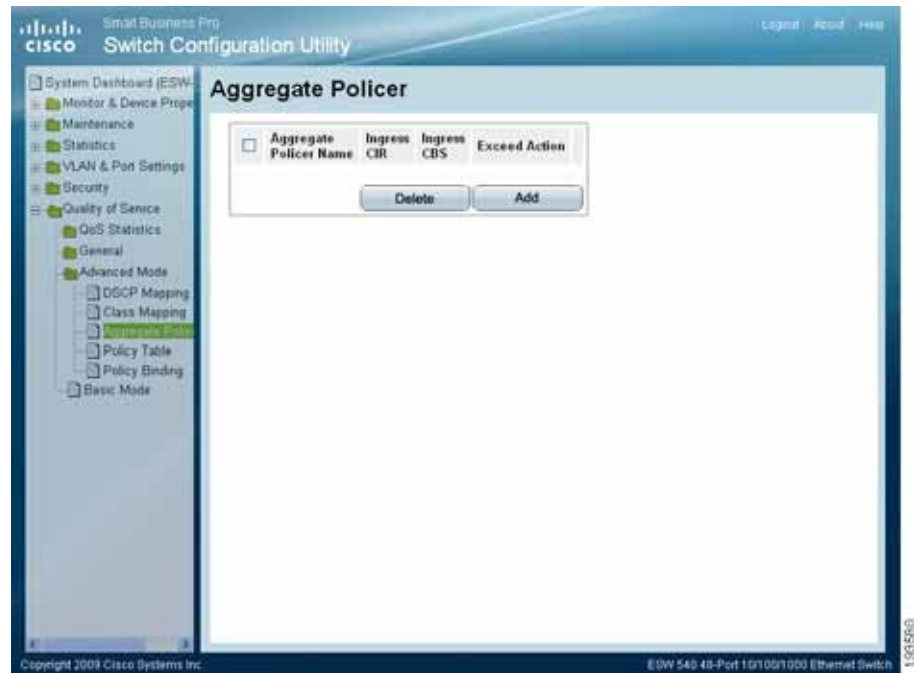
Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

To define Aggregate Policers:

- STEP 1** Click **Quality of Service > Advanced Mode > Aggregate Policer**. The *Aggregate Policer Page* opens:

#### Aggregate Policer Page

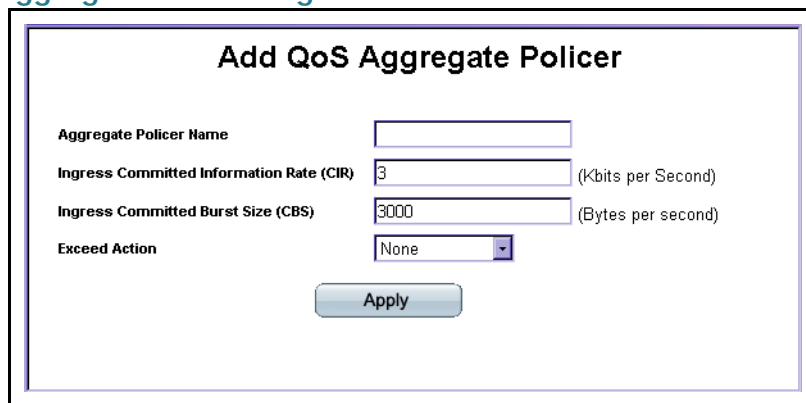


The *Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name** — Specifies the Aggregate Policer Name
- **Ingress CIR** — Defines the Committed Information Rate (CIR) in Kbits per second.
- **Ingress CbS** — Defines the Committed Burst Size (CbS) in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Remark DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.
  - *None* — Forwards packets exceeding the defined CIR value.

- STEP 2** Click the **Add** button. The *Add QoS Aggregate Policer Page* opens:

#### Add QoS Aggregate Policer Page



The screenshot shows a web form titled "Add QoS Aggregate Policer". It contains four input fields: "Aggregate Policer Name" (a text box), "Ingress Committed Information Rate (CIR)" (a text box with the value "3" and the unit "(Kbits per Second)" to its right), "Ingress Committed Burst Size (CBS)" (a text box with the value "3000" and the unit "(Bytes per second)" to its right), and "Exceed Action" (a dropdown menu with "None" selected). Below these fields is an "Apply" button.

The *Add QoS Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name** — Specifies the Aggregate Policer Name.
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbits per second.
- **Ingress Committed Burst Size (CbS)** — Defines the CbS in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Remark DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.
  - *None* — Forwards packets exceeding the defined CIR value.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The Aggregate policer is added, and the device is updated.

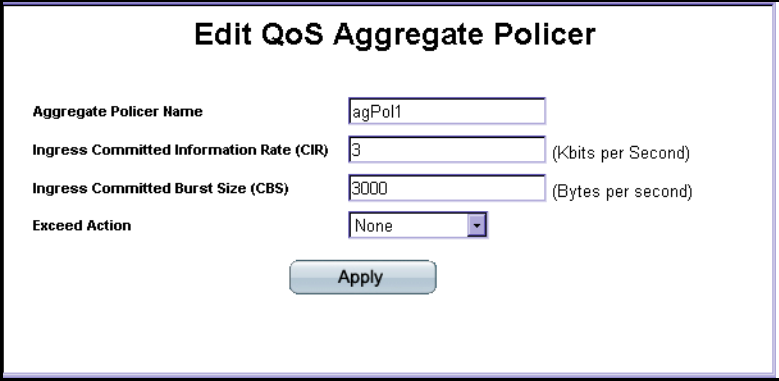
---

#### Modifying QoS Aggregate Policer

**STEP 1** Click **Quality of Service > Advanced Mode > Aggregate Policer**. The *Aggregate Policer Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit QoS Aggregate Policer Page* opens:

#### Edit QoS Aggregate Policer Page



The screenshot shows a web-based configuration page titled "Edit QoS Aggregate Policer". It contains four input fields: "Aggregate Policer Name" with the value "agPol1", "Ingress Committed Information Rate (CIR)" with the value "3" and a unit of "(Kbits per Second)", "Ingress Committed Burst Size (CBS)" with the value "3000" and a unit of "(Bytes per second)", and "Exceed Action" with a dropdown menu set to "None". An "Apply" button is located at the bottom center of the form.

The *Edit QoS Aggregate Policer Page* contains the following fields.

- **Aggregate Policer Name**— Specifies the Aggregate Policer Name
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbits per second.
- **Ingress Committed Burst Size (CbS)** — Defines the CbS in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Remark DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.
  - *None* — Forwards packets exceeding the defined CIR value.

**STEP 3** Modify the relevant fields.

**STEP 4** Click **Apply**. QoS aggregate policer settings are modified, and the device is updated.

## Configuring Policy Table

In the *Policy Table Page*, QoS policies are set up and assigned to interfaces.

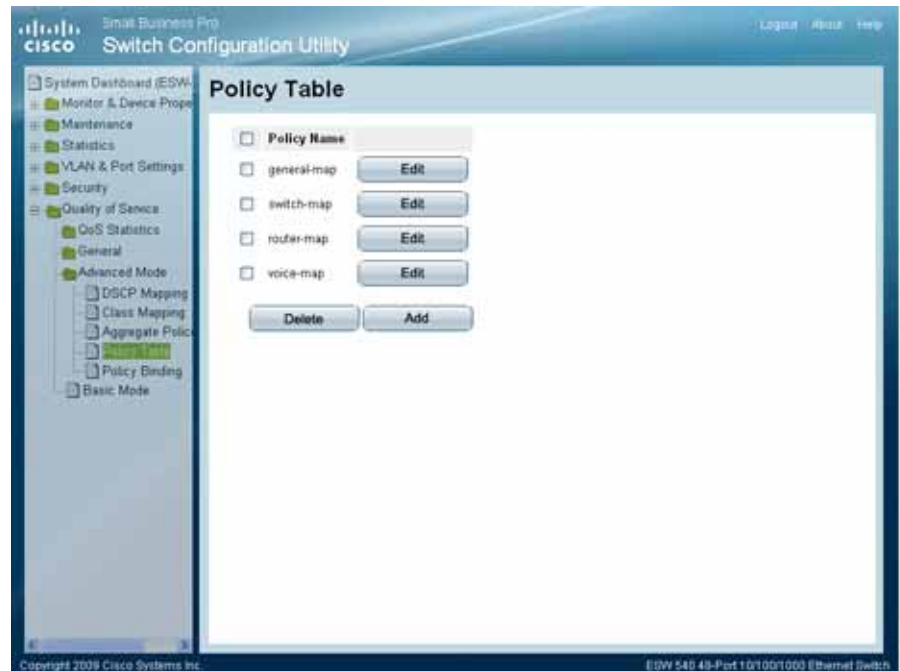
To set up QoS policies:

## Configuring Quality of Service

### Defining Advanced QoS Mode

- STEP 1** Click **Quality of Service > Advanced Mode > Policy Table**. The *Policy Table Page* opens:

#### Policy Table Page



The *Policy Table Page* contains the following field:

- **Policy Name** — Displays the user-defined policy name.

- STEP 2** Click the **Add** button. The *Add QoS Policy Profile Page* opens:

#### Add QoS Policy Profile Page

The *Add QoS Policy Profile Page* contains the following fields.

- **New Policy Name** — Specifies the user-defined policy name.
- **Class Map** — Selects the user-defined class maps which can be associated with the policy.
- **Action** — Defines the action attached to the rule. The possible field value is:
  - **Trust CoS-DSCP** — Determines the queue to which the packet is assigned dependent on the CoS tag and DSCP tag.
  - **Set** — Defines the Trust configuration manually. The possible field values are:
    - *DSCP* — In the **New Value** box, the possible values are 0-63.
    - *Queue* — In the **New Value** box, the possible values are 1-4.
    - *CoS* — In the **New Value** box, the possible values are 0-7.
- **Police** — Enables Policer functionality.
- **Type** — Policer type for the policy. Possible values are:
  - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down list. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two

different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.

- *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — Specifies the Aggregate Policer Name
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbps. This field is only relevant when the Police value is Single.
- **Ingress Committed Burst Size (CbS)** — Defines the CbS in bytes. This field is only relevant when the Police value is Single.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Out of Profile DSCP* — Remarks packet's DSCP values exceeding the defined CIR value.
  - *None* — Forwards packets exceeding the defined CIR value.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The QoS policy profile is added, and the device is updated.

---

### Modifying the QoS Policy Profile

---

**STEP 1** Click **Quality of Service > Advanced Mode > QoS Policy Profile**. The *Policy Table Page* opens.

**STEP 2** Click the **Edit** button. The *Edit QoS Policy Profile Page* opens:

#### Edit QoS Policy Profile Page

The *Edit QoS Policy Profile Page* contains the following fields.

- **Policy Name** — Displays the user-defined policy name.
- **Class Map** — Displays the user-defined name of the class map.
- **Action** — Defines the action attached to the rule. The possible field value is:
  - **Trust CoS-DSCP** — Determines the queue to which the packet is assigned dependent on the CoS tag and DSCP tag.
  - **Set** — Defines the Trust configuration manually. The possible field values are:
    - *DSCP* — In the **New Value** box, the possible values are 0-63.
    - *Queue* — (applicable only to Gigabyte devices)
    - *CoS* — In the **New Value** box, the possible values are 0-7. (applicable only to Gigabyte devices)
- **Police** — Enables Policer functionality.



- **Type** — Policer type for the policy. Possible values are:
  - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down list. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
  - *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — Specifies the Aggregate Policer Name
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbps. This field is only relevant when the Police value is Single.
- **Ingress Committed Burst Size (CbS)** — Defines the CbS in bytes. This field is only relevant when the Police value is Single.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
  - *Drop* — Drops packets exceeding the defined CIR value.
  - *Out Of Profile DSCP* —Remarks packet's DSCP values exceeding the defined CIR value.
  - *None* —Forwards packets exceeding the defined CIR value.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The QoS policy profile is modified, and the device is updated.

---

## Defining Policy Binding

In the *Policy Binding Page*, QoS policies are associated with specific interfaces.

## Configuring Quality of Service

### Defining Advanced QoS Mode

- STEP 1** Click **Quality of Service > Advanced Mode > Policy Binding**. The *Policy Binding Page* opens:

#### Policy Binding Page

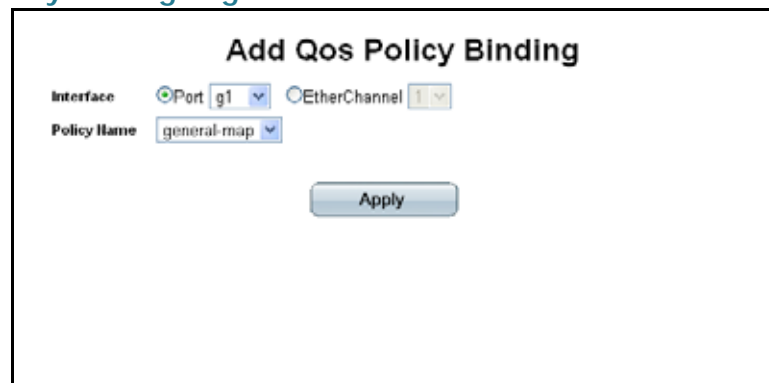


The *Policy Binding Page* contains the following fields:

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Displays a Policy name associated with the interface.

- STEP 2** Click the **Add** button. The *Add QoS Policy Binding Page* opens:

#### Add QoS Policy Binding Page



The *Add QoS Policy Binding Page* contains the following fields.

- **Interface** — Select either the Port or EtherChannel radio button to select the interface.
- **Policy Name** — Select a Policy to associate with the interface.

**STEP 3** Define the relevant fields.

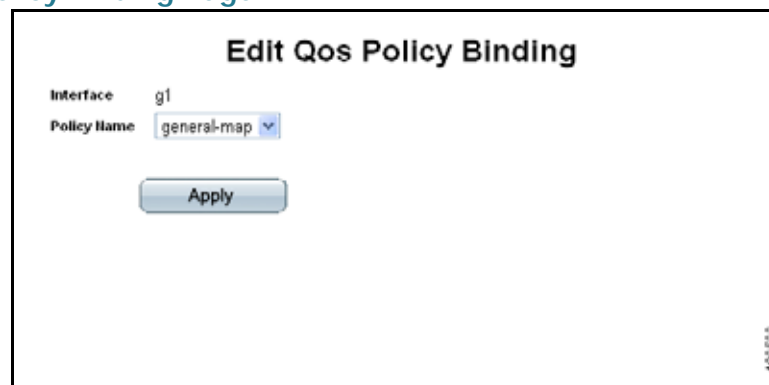
**STEP 4** Click **Apply**. The QoS Policy Binding is defined, and the device is updated.

#### Modifying QoS Policy Binding Settings

**STEP 1** Click **Quality of Service > Advanced Mode > Policy Binding**. The *Policy Binding Page* opens:

**STEP 2** Click the **Edit** button. The *Edit QoS Policy Binding Page* opens:

#### Edit QoS Policy Binding Page



The *Edit QoS Policy Binding Page* contains the following fields.

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Displays the Policy name associated with the interface.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The QoS policy binding is modified, and the device is updated.

## Defining QoS Basic Mode

The *Basic Mode Page* contains information for enabling Trust on the device. Packets entering a QoS domain are classified at the edge of the QoS domain.

To define the Trust configuration:

**STEP 1** Click **Quality of Service > Basic Mode**. The *Basic Mode Page* opens:

### Basic Mode Page



The *Basic Mode Page* contains the following fields:

- **Trust Mode** — Displays the trust mode. If a packet's CoS tag and DSCP tag, are mapped to different queues, the Trust Mode determines the queue to which the packet is assigned. Possible values are:
  - *CoS* — Sets trust mode to CoS on the device. The CoS mapping determines the packet queue
  - *DSCP* — Sets trust mode to DSCP on the device. The DSCP mapping determines the packet queue.
- **Always Rewrite DSCP** — Rewrites the packet DSCP tag according to the QoS DSCP Rewriting configuration. *Always Rewrite DSCP* can only be selected if the Trust Mode is set to *DSCP*.

### Rewriting DSCP Values

In the *DSCP Mapping Page*, define the Differentiated Services Code Point (DSCP) tag to use in place of the incoming DSCP tags.

**STEP 2** Click **DSCP Rewrite**. The *DSCP Mapping Page* opens:

#### DSCP Mapping Page

### DSCP Mapping

DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0	16	16	32	32	48	48
1	1	17	17	33	33	49	49
2	2	18	18	34	34	50	50
3	3	19	19	35	35	51	51
4	4	20	20	36	36	52	52
5	5	21	21	37	37	53	53
6	6	22	22	38	38	54	54
7	7	23	23	39	39	55	55
8	8	24	24	40	40	56	56
9	9	25	25	41	41	57	57
10	10	26	26	42	42	58	58
11	11	27	27	43	43	59	59
12	12	28	28	44	44	60	60
13	13	29	29	45	45	61	61
14	14	30	30	46	46	62	62
15	15	31	31	47	47	63	63

The *DSCP Mapping Page* contains the following fields:

- **DSCP In** — Indicates the DSCP value in the incoming packet.
- **DSCP Out** — Indicates the DSCP value in the outgoing packet.

**STEP 3** Define the DSCP mappings.

**STEP 4** Click **Apply**. The DSCP mappings are defined, and the device is updated.

# Configuring SNMP

The Simple Network Management Protocol (SNMP) provides a method for managing network devices.

## SNMP Versions

The device supports the following SNMP versions:

### SNMP v1 and v2

SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agents are controlled by access strings.

### SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against disclosure message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on a SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares the incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use. The device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

The device generates the following trap:

- Copy trap

The SNMP section contains the following topics:

- Configuring SNMP Security
- Defining Trap Management

## Configuring SNMP Security

The Security section contains the following topics:

- Defining the SNMP Engine ID
- Defining SNMP Views
- Defining SNMP Users
- Define SNMP Groups
- Defining SNMP Communities

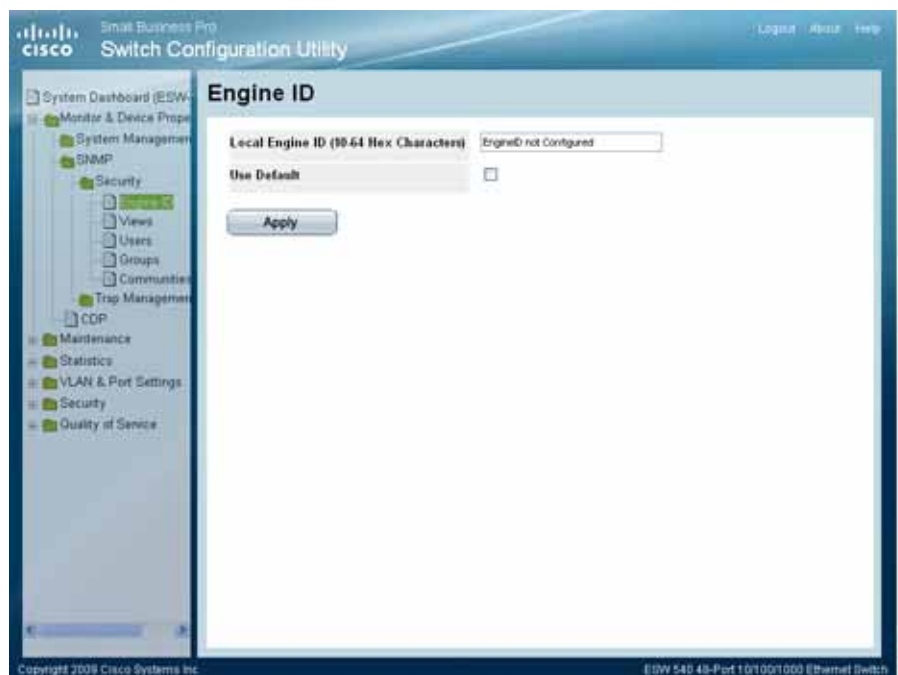
### Defining the SNMP Engine ID

The *Engine ID Page* provides information for defining the device engine ID. The Engine ID must be defined before SNMPv3 is enabled. Select a default Engine ID that is comprised of Enterprise number and the default MAC address. Verify that the Engine ID is unique for the administrative domain. This prevents two devices in a network from having the same Engine ID.



- STEP 1** Click **Monitor & Device Properties > SNMP > Security > Engine ID**. The *Engine ID Page* opens:

#### Engine ID Page



The *Engine ID Page* contains the following fields.

- **Local Engine ID (10-64 Hex characters)** — Indicates the local device engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings consists of two hexadecimal digits.
- **Use Default** — Uses the device generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:
  - *First 4 octets* — first bit = 1, the rest is IANA Enterprise number.
  - *Fifth octet* — Set to 3 to indicate the MAC address that follows.
  - *Last 6 octets* — MAC address of the device.

The possible values are:

- *Checked* — Use the default Engine ID.
- *Unchecked* — Use a user-defined Engine ID.

- STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The SNMP Engine ID is defined, and the device is updated.

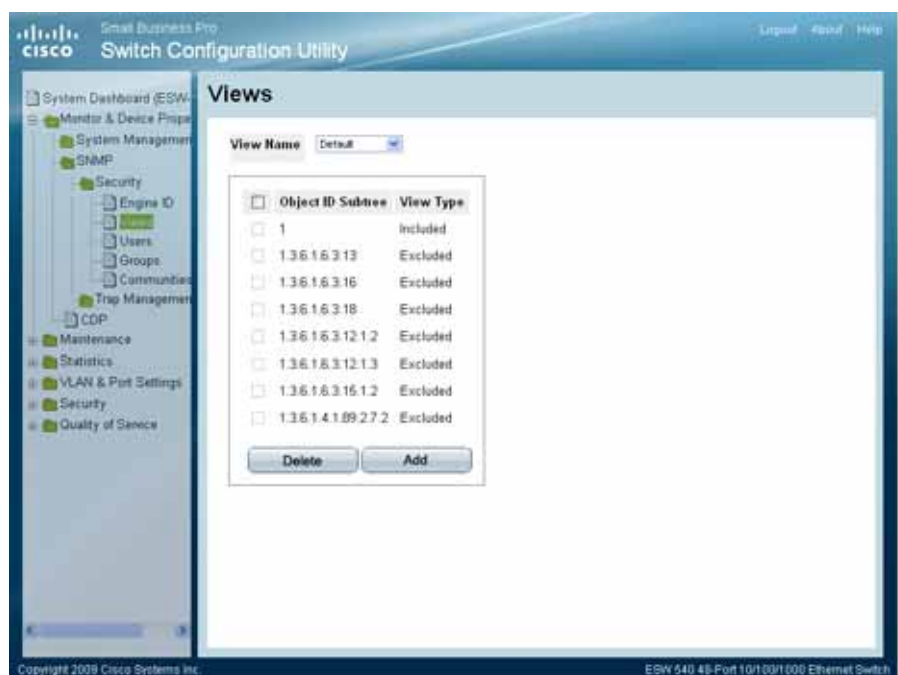
## Defining SNMP Views

SNMP Views provide access or block access to device features or feature aspects. For example, a view displays that the SNMP Group A has Read Only (R/O) access to Multicast groups, while SNMP Group B has Read-Write (R/W) access to Multicast groups. Feature access is granted via the MIB name, or MIB Object ID.

To define SNMP views:

**STEP 1** Click **Monitor & Device Properties > SNMP > Security > Views**. The *SNMP Views Page* opens:

### SNMP Views Page



The *SNMP Views Page* contains the following fields:

- **View Name** — Displays the user-defined views. The options are as follows:
  - *Default* — Displays the default SNMP view for read and read/write views.
  - *DefaultSuper* — Displays the default SNMP view for administrator views.

- **Object ID Subtree** — Indicates the device feature OID that is included or excluded in the selected SNMP view.
- **View Type** — Indicates if the defined OID branch that are included or excluded in the selected SNMP view.

**STEP 2** Click the **Add** button. The *Add SNMP View Page* opens:

#### Add SNMP View Page

The screenshot shows the 'Add SNMP View' configuration page. It includes a 'View Name' text field, an 'Object ID Subtree' section with a 'Select from List' button, a list of subnets (system, interfaces, ip, icmp, tcp), 'Up' and 'Down' buttons, and an 'Insert' radio button next to a text input field containing '1.3.6.1.2.1.1'. The 'View Type' is set to 'Included'. An 'Apply' button is at the bottom right.

The *Add SNMP View Page* contains parameters for defining and configuring new SNMP view. The *Add SNMP View Page* contains the following fields:

- **View Name** — Defines the user-defined view name.
- **Object ID Subtree** — Indicates the device feature OID included or excluded in the selected SNMP view. The options to select the Object are as follows:
  - *Select from List* — Select the Subtree from the list provided. Pressing the *Up* and *Down* buttons allows you to change the priority by moving the selected subtree up or down in the list.
  - *Insert* — Enables a Subtree not included to be entered.
- **View Type** — Indicates if the defined OID branch will be included or excluded in the selected SNMP view. The options to select the Subtree are as follows:
  - *Included* — Includes the defined OID branch.
  - *Excluded* — Excludes the defined OID branch.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNMP views are defined, and the device is updated.

## Defining SNMP Users

The *SNMP Users Page* provides information for creating SNMP users, and assigning SNMP access control privileges to SNMP users. Groups allow network managers to assign access rights to specific device features, or feature aspects.

- STEP 1** Click **Monitor & Device Properties > SNMP > Security > Users**. The *SNMP Users Page* opens:

### SNMP Users Page



The *SNMP Users Page* contains the following fields.

- **User Name** — Displays the user-defined user name to which access control rules are applied. The field range is up to 30 characters.
- **Group Name** — User-defined SNMP group to which the SNMP user belongs. SNMP groups are defined in the *SNMP Group Profile Page*.



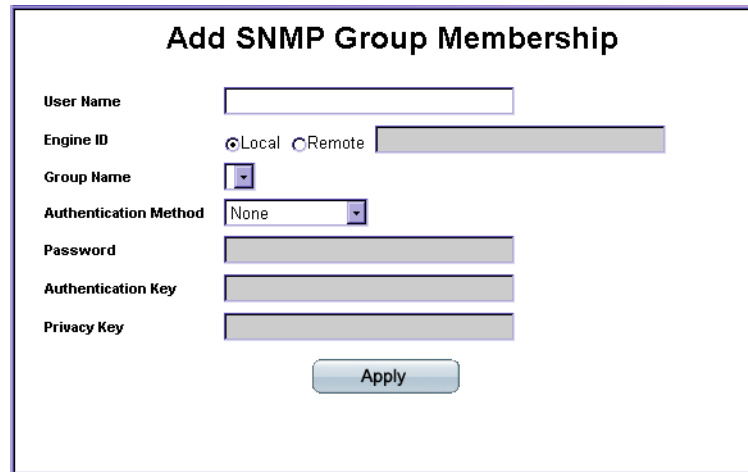
**NOTE** Users can only be added to groups that have been provisioned with SNMPv3.

- **Engine ID** — Indicates the local/remote device engine ID.

- **Authentication** — Indicates the Authentication method used.

**STEP 2** Click the **Add** button. The *Add SNMP Group Membership Page* opens:

### Add SNMP Group Membership Page



The Add SNMP Group Membership Page provides information for assigning SNMP access control privileges to SNMP groups. The *Add SNMP Group Membership Page* contains the following fields.

- **User Name** — Provides a user-defined local user list.
- **Engine ID** — Indicates either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 User Database.
  - *Local* — Indicates that the user is connected to a local SNMP entity.
  - *Remote* — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.
- **Group Name** — Contains a list of SNMP groups to which the SNMP user belongs. SNMP groups are defined in the *SNMP Group Profile Page*.
- **Authentication Method** — Indicates the Authentication method used. The possible field values are:
  - *MD5 Key* — Users are authenticated using a valid HMAC-MD5 key.
  - *SHA Key* — Users are authenticated using a valid HMAC-SHA-96 key.
  - *MD5 Password* — Users should enter a password that is encrypted using the HMAC-MD5-96 authentication method.

## Configuring SNMP

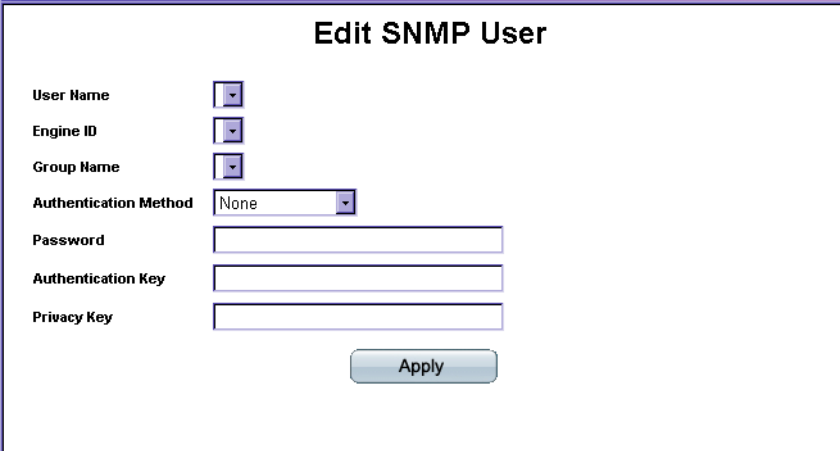
### Configuring SNMP Security

- *SHA Password* — Users should enter a password that is encrypted using the HMAC-SHA-96 authentication method.
  - *None* — No user authentication is used.
- **Password** — Define the local user password. Local user passwords can contain up to 159 characters. This field is available if the Authentication Method is a password.
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If HMAC-MD5-96 is selected then 16 bytes are required and if HMAC-SHA-96 then 20 bytes are required. This field is available if the Authentication Method is a key.
- **Privacy Key** — Defines the Privacy Key (LSB). If only authentication is required, 16\20 bytes are defined. If both privacy and authentication are required, 36\40 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. This field is available if the Authentication Method is a key.

### Modifying SNMP Users

The Edit SNMP User Page provides information for assigning SNMP access control privileges to SNMP groups.

#### Edit SNMP User Page



The screenshot shows the 'Edit SNMP User' configuration page. It contains several fields for user configuration:

- User Name**: A dropdown menu.
- Engine ID**: A dropdown menu.
- Group Name**: A dropdown menu.
- Authentication Method**: A dropdown menu currently set to 'None'.
- Password**: A text input field.
- Authentication Key**: A text input field.
- Privacy Key**: A text input field.
- Apply**: A button at the bottom right.

The Edit SNMP User Page contains the following fields.

- **User Name** — Displays the user-defined group to which access control rules are applied. Provides a user-defined local user list.
- **Engine ID** — Indicates the local device engine ID.

- **Group Name** — SNMP group, which can be chosen from the list, to which the SNMP user belongs. SNMP groups are defined in the SNMP Group Profile page.
- **Authentication Method** — Indicates the Authentication method used. The possible field values are:
  - *MD5 Key* — Users are authenticated using a valid HMAC-MD5 key.
  - *SHA Key* — Users are authenticated using a valid HMAC-SHA-96 key.
  - *MD5 Password* — Users should enter a password that is encrypted using the HMAC-MD5-96 authentication method.
  - *SHA Password* — Users should enter a password that is encrypted using the HMAC-SHA-96 authentication method.
  - *None* — No user authentication is used.
- **Password** — Define the local user password. Local user passwords can contain up to 159 characters. This field is available if the Authentication Method is a password.
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. This field is available if the Authentication Method is a key.
- **Privacy Key** — Defines the Privacy Key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon. This field is available if the Authentication Method is a key.

**STEP 3** Define the relevant fields.

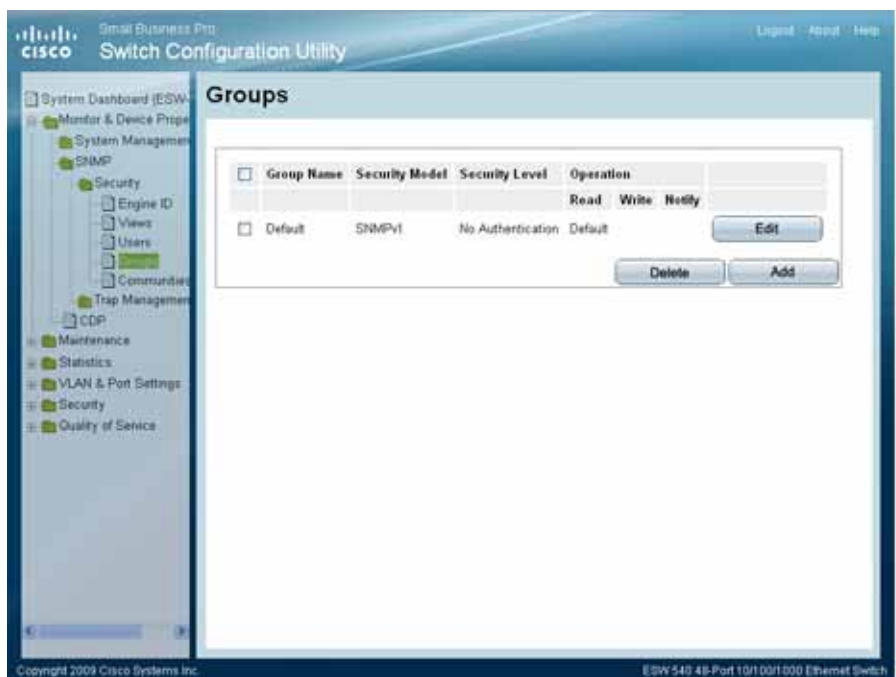
**STEP 4** Click **Apply**. The SNMP User is modified, and the device is updated.

## Define SNMP Groups

The *SNMP Groups Page* provides information for creating SNMP groups and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or features aspects.

- STEP 1** Click **Monitor & Device Properties > SNMP > Security > Groups**. The *SNMP Groups Page* opens:

#### SNMP Groups Page



The *SNMP Groups Page* contains the following fields:

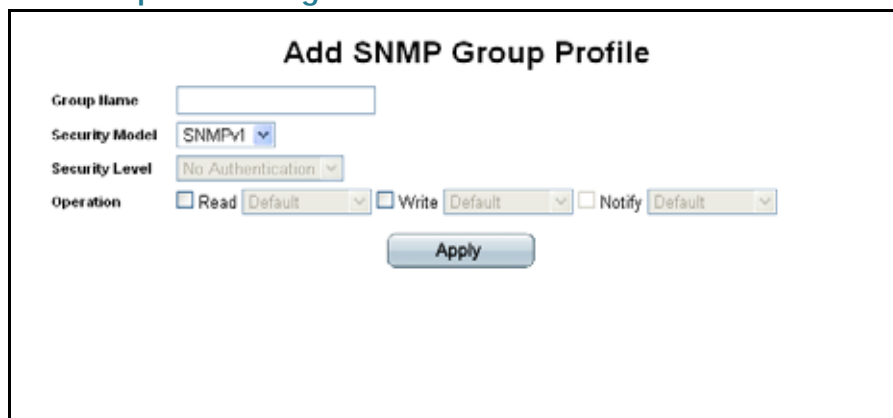
- **Group Name** — Displays the user-defined group to which privileges are applied.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 is defined for the group.
  - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:
  - *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication* — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.



- *Privacy* — Encrypts SNMP message.
- **Operation** — Defines the group access right, which are per view. The possible field values are:
  - *Read* — The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  - *Write* — The management access is read-write and changes can be made to the assigned SNMP view.
  - *Notify* — Sends traps for the assigned SNMP view.

**STEP 2** Click the **Add** button. The *Add SNMP Group Profile Page* opens:

#### Add SNMP Group Profile Page



The *Add SNMP Group Profile Page* allows network managers to define new SNMP Group profiles. The *Add SNMP Group Profile Page* contains the following fields:

- **Group Name** — Defines the user-defined group to which privileges are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 is defined for the group.
  - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only. The possible field values are:

## Configuring SNMP

### Configuring SNMP Security

- *No Authentication* — Neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication* — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
  - *Privacy* — Encrypts SNMP message.
- **Operation** — Defines the group access right, which are per view. The possible field values are:
  - *Default* — Defines the default group access rights.
  - *DefaultSuper* — Defines the default group access rights for administrator.
  - *Read* — The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  - *Write* — The management access is read-write and changes can be made to the assigned SNMP view.
  - *Notify* — Sends traps for the assigned SNMP view.

### Modifying SNMP Group Profile Settings

**STEP 1** Click **Monitor & Device Properties > SNMP > Security > Groups**. The *SNMP Groups Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit SNMP Group Profile Page* opens:

#### Edit SNMP Group Profile Page

**Edit SNMP Group Profile**

Group Name:

Security Model:

Security Level:

Operation: ☒ Read  ☐ Write  ☐ Notify

The *Edit SNMP Group Profile Page* contains the following fields:

- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  - *SNMPv1* — SNMPv1 is defined for the group.
  - *SNMPv2* — SNMPv2 is defined for the group.
  - *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only.
  - *No Authentication* — Neither the Authentication nor the Privacy security levels are assigned to the group.
  - *Authentication* — Authenticates SNMP messages, and ensures the SNMP messages origin is authenticated.
  - *Privacy* — Encrypts SNMP message.
- **Operation** — Defines the group access rights. The options for Read, Write, and Notify operations are as follows:
  - *Default* — Defines the default group access rights.
  - *DefaultSuper* — Defines the default group access rights for administrator.
  - *Read* — The management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  - *Write* — The management access is read-write and changes can be made to the assigned SNMP view.
  - *Notify* — Sends traps for the assigned SNMP view.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNMP Group Profile is modified, and the device is updated.

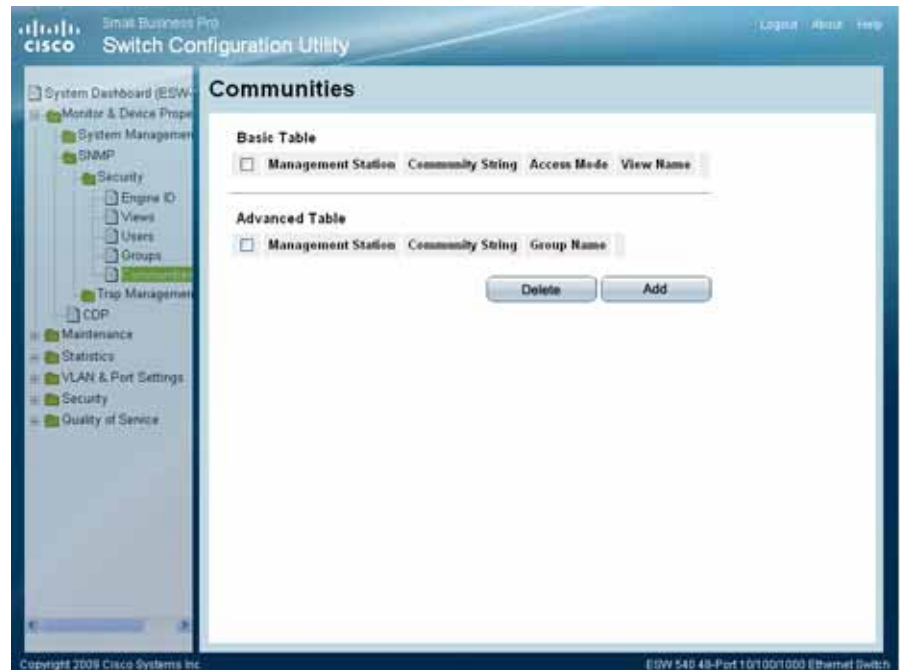
## Defining SNMP Communities

The Access rights are managed by defining communities in the *SNMP Communities Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

To define SNMP Communities:

- STEP 1** Click **Monitor & Device Properties > SNMP > Security > Communities**. The *SNMP Communities Page* opens:

### SNMP Communities Page



The *SNMP Communities Page* is divided into the following tables:

- Basic Table
- Advanced Table

The SNMP Communities Basic Table area contains the following fields:

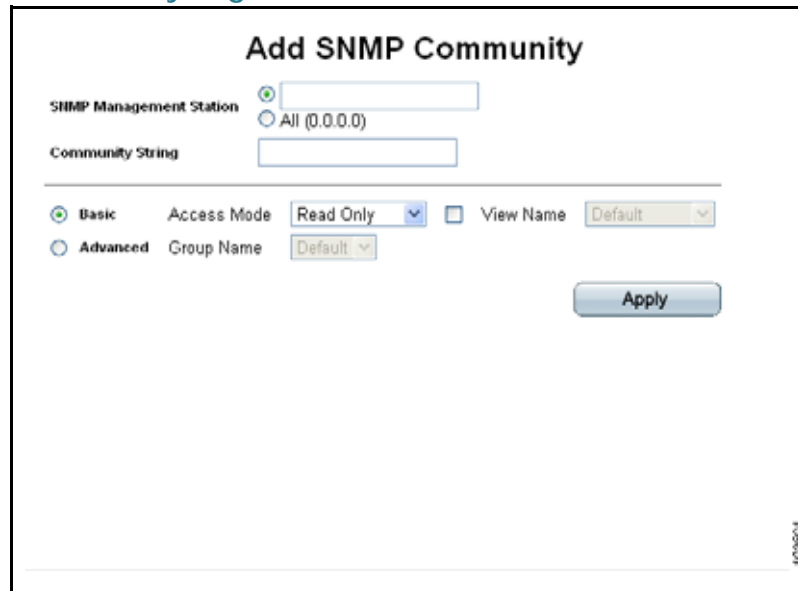
- **Management Station** — Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** — Displays the password used to authenticate the management station to the device.
- **Access Mode** — Displays the access rights of the community.
- **View Name** — Displays the SNMP view.

The SNMP Communities Advanced Table area contains the following fields:

- **Management Station** — Displays the management station IP address for which the Advanced SNMP community is defined.
- **Community String** — Displays the password used to authenticate the management station to the device.
- **Group Name** — Displays advanced SNMP communities group name.

**STEP 2** Click the **Add** button. The *Add SNMP Community Page* opens.

#### Add SNMP Community Page



The screenshot shows the 'Add SNMP Community' configuration page. It features two radio buttons for 'SNMP Management Station': 'Basic' (selected) and 'All (0.0.0.0)'. Below these is a text field for 'Community String'. A horizontal separator line divides the page into two sections. The top section is for 'Basic' mode, with a radio button selected, an 'Access Mode' dropdown menu set to 'Read Only', and a 'View Name' dropdown menu set to 'Default'. The bottom section is for 'Advanced' mode, with a radio button unselected and a 'Group Name' dropdown menu set to 'Default'. An 'Apply' button is located at the bottom right of the form.

The *Add SNMP Community Page* allows network managers to define and configure new SNMP communities. The *Add SNMP Community Page* contains the following fields:

- **SNMP Management Station** — Defines the management station IP address for which the SNMP community is defined. There are two definition options:
  - Define the management station IP address.
  - *All*, which includes all management station IP addresses.
- **Community String** — Defines the password used to authenticate the management station to the device.

Configure either the Basic Mode or the Advanced Mode.

- **Basic** — Enables SNMP Basic mode for a selected community and contains the following fields:

- **Access Mode** — Defines the access rights of the community. The possible field values are:
  - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
  - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
  - *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
- **View Name** — Contains a list of user-defined SNMP views.
- **Advanced** — Enables SNMP Advanced mode for a selected community and contains the following field:
  - **Group Name** — Defines advanced SNMP communities group names.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNMP Community is defined, and the device is updated.

## Modifying SNMP Community Settings

**STEP 1** Click **Monitor & Device Properties > SNMP > Security > Communities**. The *SNMP Communities Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit SNMP Community Page*:

### Edit SNMP Community Page



The screenshot shows the 'Edit SNMP Community' configuration window. It has a title bar 'Edit SNMP Community'. Inside, there are two dropdown menus: 'SNMP Management' with the value '1.1.1.1' and 'Community String' with the value 'ComString1'. Below these is a horizontal separator line. Under the line, there are two radio buttons: 'Basic' (selected) and 'Advanced'. To the right of the 'Basic' radio button, there is an 'Access Mode' dropdown menu with 'Read Only' selected, and a checked checkbox labeled 'View Name' followed by a dropdown menu with 'Default' selected. To the right of the 'Advanced' radio button, there is a 'Group Name' dropdown menu with 'gr2' selected. At the bottom center of the window is an 'Apply' button.

The *Edit SNMP Community Page* contains the following fields:

- **SNMP Management** — Defines the management station IP address for which the SNMP community is defined.

- **Community String** — Defines the password used to authenticate the management station to the device.

Configure either the Basic Mode or the Advanced Mode.

- **Basic** — Enables SNMP Basic mode for a selected community and contains the following fields:
- **Access Mode** — Defines the access rights of the community. The possible field values are:
  - *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
  - *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
  - *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
- **View Name** — Contains a list of user-defined SNMP views.
- **Advanced** — Enables SNMP Advanced mode for a selected community and contains the following fields:
  - **Group Name** — Defines advanced SNMP communities group names.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNMP Community settings are defined, and the device is updated.

## Defining Trap Management

This section contains the following topics:

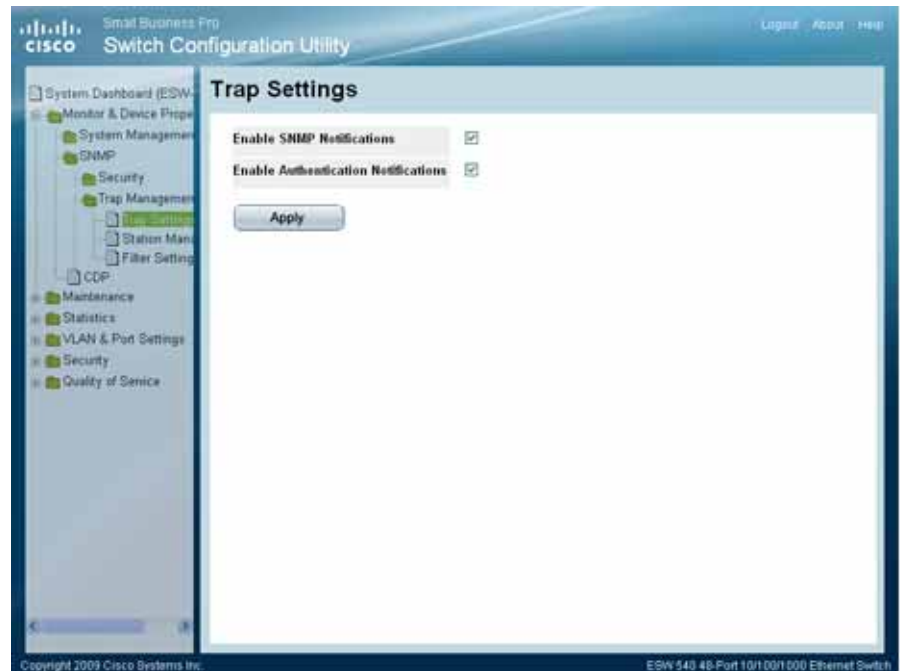
- Defining Trap Settings
- Configuring Station Management
- Defining SNMP Filter Settings

### Defining Trap Settings

The *Trap Settings Page* contains parameters for defining SNMP notification parameters.

- STEP 1** Click **Monitor & Device Properties > SNMP > Trap Management > Trap Settings**. The *Trap Settings Page* opens:

#### Trap Settings Page



The *Trap Settings Page* contains the following fields:

- **Enable SNMP Notification** — Specifies whether the device can send SNMP notifications. The possible field values are:
  - *Checked* — Enables SNMP notifications.
  - *Unchecked* — Disables SNMP notifications.
- **Enable Authentication Notification** — Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
  - *Checked* — Enables the device to send authentication failure notifications.
  - *Unchecked* — Disables the device from sending authentication failure notifications.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. The SNMP Trap settings are defined, and the device is updated.



## Configuring Station Management

The *Station Management Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

Traps indicating status changes are issued by the switch to specified trap managers. Specify the trap managers so that key events are reported by this switch to the management station. Specify up to eight management stations that receive authentication failure messages and other trap messages from the switch.

**STEP 1** Click **Monitor & Device Properties > SNMP > Trap Management > Station Management**. The *Station Management Page* opens:

### Station Management Page



The *Station Management Page* contains two areas, the *SNMPv1,2 Notification Recipient* and the *SNMPv3 Notification Recipient* table.

The *SNMPv1,2 Notification Recipient* table area contains the following fields:

- **Recipients IP** — Indicates the IP address to which the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
  - *Trap* — Indicates traps are sent.
  - *Inform* — Indicates informs are sent.
- **Community String** — Identifies the community string of the trap manager.
- **Notification Version** — Determines the trap type. The possible field values are:
  - *SNMP V1* — Indicates SNMP Version 1 traps are sent.
  - *SNMP V2* — Indicates SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 attempts.

The *SNMPv3 Notification Recipient* table area contains the following fields:

- **Recipients IP** — Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
  - *Trap* — Indicates traps are sent.
  - *Inform* — Indicates informs are sent.
- **User Name** — Displays the SNMP user names.
- **Security Level** — Defines the means by which the packet is authenticated. The possible field values are:
  - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
  - *Authentication* — Indicates the packet is authenticated.
  - *Privacy* — Indicates the packet is both authenticated and encrypted.

- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Defines if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 attempts.

**STEP 2** Click the **Add** button. The *Add SNMP Notification Recipient Page* opens.

#### Add SNMP Notification Recipient Page

The screenshot shows the 'Add SNMP Notification Recipient' configuration page. It contains the following fields and options:

- Recipient IP Address**: A text input field.
- Notification Type**: A dropdown menu with 'Traps' selected.
- SNMPv1,2** section (selected with a radio button):
  - Community String**: A text input field.
  - Notification Version**: A dropdown menu with 'SNMPv1' selected.
- SNMPv3** section (unselected with a radio button):
  - User Name**: A text input field.
  - Security Level**: A dropdown menu with 'NoAuthentication' selected.
- UDP Port**: A text input field with '162' entered.
- Filter Name**: A dropdown menu.
- Timeout**: A text input field with '15' entered, followed by '(Sec)'.
- Retries**: A text input field with '3' entered.
- Apply**: A button at the bottom right.

The *Add SNMP Notification Recipient Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters

- Providing Access Control Checks

The *Add SNMP Notification Recipient Page* contains the following fields:

- **Recipient IP Address**— Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
  - *Trap* — Indicates traps are sent.
  - *Inform* — Indicates informs are sent.

Either SNMPv1,2 or SNMPv3 may be used as the version of traps, with only one version enabled at a single time.

The SNMPv1,2 Notification Recipient area contains the following fields:

- **SNMPv1,2** — Enables SNMPv1,2 as the Notification version. If SNMPv1,2 is enabled, the **Community String** and **Notification Version** fields are enabled for configuration:
- **Community String** — Identifies the community string of the trap manager.
- **Notification Version** — Determines the trap type. The possible field values are:
  - *SNMP V1* — Indicates SNMP Version 1 traps are sent.
  - *SNMP V2* — Indicates SNMP Version 2 traps are sent.

The SNMPv3 Notification Recipient area contains the following fields:

- **SNMPv3** — Enables SNMPv3 as the Notification version. If SNMPv3 is enabled, the **User Name** and **Security Level** fields are enabled for configuration:
- **User Name** — Defines the user to whom SNMP notifications are sent.
- **Security Level** — Defines the means by which the packet is authenticated. The possible field values are:
  - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
  - *Authentication* — Indicates the packet is authenticated.
  - *Privacy* — Indicates the packet is both authenticated and encrypted.

The UDP Port Notification Recipient area contains the following fields:

- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.

## Configuring SNMP

### Defining Trap Management

---

- **Filter Name** — Defines if the SNMP filter for which the SNMP Notification filter is defined.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 attempts.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNMP Notification Recipient settings are defined, and the device is updated.

## Modifying SNMP Notifications

The *Edit SNMP Notification Recipient Page* allows system administrators to define notification settings. The *Edit SNMP Notification Recipient Page* is divided into four areas, Notification Recipient, SNMPv1,2 Notification Recipient, SNMPv3 Notification Recipient and UDP Port Notification Recipient.

---

**STEP 1** Click **Monitor & Device Properties > SNMP > Trap Management > Station Management**.

**STEP 2** Click the **Edit** button. The *Edit SNMP Notification Recipient Page* opens:

## Edit SNMP Notification Recipient Page

The screenshot shows the 'Edit SNMP Notification Recipient' configuration page. It features several sections for configuring SNMP traps and informs. The top section includes 'Recipient IP Address' (1.1.1.1) and 'Notification Type' (Traps). Below this, there are two main sections: 'SNMPv1,2' and 'SNMPv3'. The 'SNMPv1,2' section is active, showing 'Community String' (ComStr3) and 'Notification Version' (SNMPv1). The 'SNMPv3' section shows 'User Name' and 'Security Level' (NoAuthentication). At the bottom, there are fields for 'UDP Port' (162), 'Filter Name', 'Informs Timeout' (15), and 'Informs Retries' (3). An 'Apply' button is located at the bottom right.

Edit SNMP Notification Recipient	
Recipient IP Address	1.1.1.1
Notification Type	Traps
<hr/>	
SNMPv1,2	
Community String	ComStr3
Notification Version	SNMPv1
<hr/>	
SNMPv3	
User Name	
Security Level	NoAuthentication
<hr/>	
UDP Port	162
Filter Name	
Informs Timeout	15
Informs Retries	3
<div>Apply</div>	

The *Edit SNMP Notification Recipient Page* contains the following fields:

- **Recipient IP Address** — Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
  - *Trap* — Indicates traps are sent.
  - *Inform* — Indicates informs are sent.

Either SNMPv1,2 or SNMPv3 may be used as the version of traps, with only one version enabled at a single time. The SNMPv1,2 Notification Recipient area contains the following fields:

- **SNMPv1,2** — Enables SNMPv1,2 as the Notification version. If SNMPv1,2 is enabled, the **Community String** and **Notification Version** fields are enabled for configuration:
- **Community String** — (SNMP v1, 2) Identifies the community string of the trap manager.
- **Notification Version** — (SNMP v1, 2) Determines the trap type. The possible field values are:

- *SNMP V1* — Indicates SNMP Version 1 traps are sent.
- *SNMP V2* — Indicates SNMP Version 2 traps are sent.

The SNMPv3 Notification Recipient area contains the following fields:

- **SNMPv3** — Enables SNMPv3 as the Notification version. If SNMPv3 is enabled, the **User Name** and **Security Level** fields are enabled for configuration:
- **User Name** — Defines the user to whom SNMP notifications are sent.
- **Security Level** — (SNMP v3) Defines the means by which the packet is authenticated. The possible field values are:
  - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
  - *Authentication* — Indicates the packet is authenticated.
  - *Privacy* — Indicates the packet is both authenticated and encrypted.

The UDP Port Notification Recipient area contains the following fields:

- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- **Informs Timeout** — Indicates the amount of time (seconds) the device waits before re-sending informs. The default is 15 seconds.
- **Informs Retries** — Indicates the amount of times the device re-sends an inform request. The default is 3 attempts.

**STEP 3** Define the relevant fields.

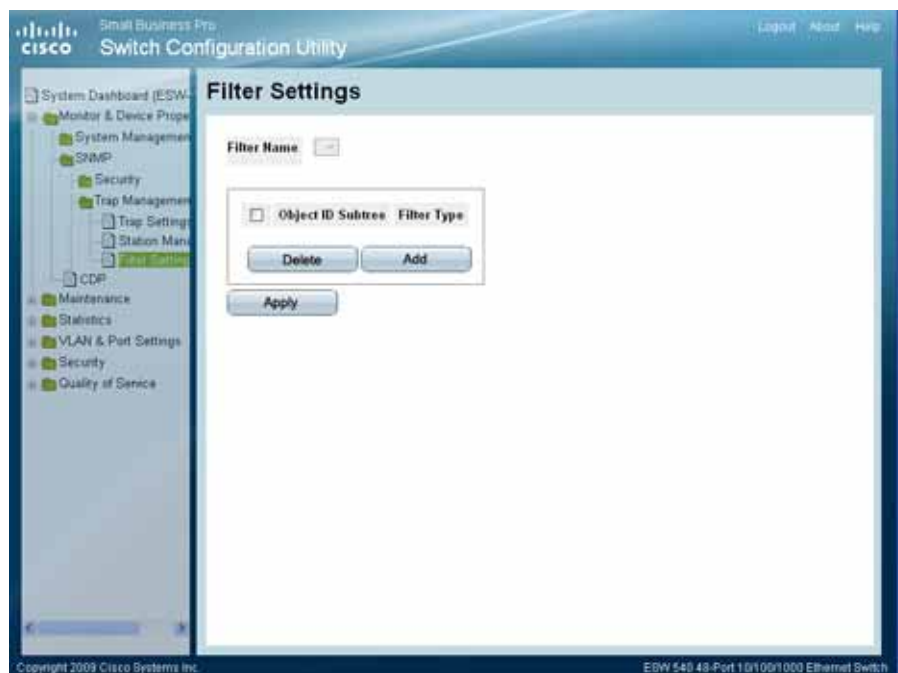
**STEP 4** Click **Apply**. The SNMP Notification Receivers are modified, and the device is configured.

## Defining SNMP Filter Settings

The Filter Settings Page permits filtering traps based on OIDs. Each OID is linked to a device feature or a feature aspect. The Filter Settings Page also allows network managers to filter notifications.

- STEP 1** Click **Monitor & Device Properties > SNMP > Trap Management > Filter Settings**. The *Filter Settings Page* opens:

#### Filter Settings Page



The *Filter Settings Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **Object ID Subtree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients.
- **Filter Type** — Indicates whether informs or traps are sent regarding the OID to the trap recipients.
  - *Excluded* — Restricts sending OID traps or informs.
  - *Included* — Sends OID traps or informs.

- STEP 2** Click the **Add** button. The *Add SNMP Notification Filter Page* opens:



### Add SNMP Notification Filter Page

The screenshot shows the 'Add SNMP Notification Filter' window. It includes a 'Filter Name' text box, a 'New Object Identifier Tree' section with a 'Select from List' radio button and a list box containing 'interfaces', 'ip', 'icmp', 'tcp', and 'udp', and 'Up'/'Down' buttons. There is also an 'Object ID' radio button and text box. The 'Filter Type' is set to 'Included'. An 'Apply' button is at the bottom.

The *Add SNMP Notification Filter Page* contains the following fields:

- **Filter Name** — Defines notification filters.
- **New Object Identifier Tree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are selected from either the *Select from List* or the *Object ID List*. There are two configuration options:
  - *Select from List* — Select the OID from the list provided. Pressing the *Up* and *Down* buttons allows you to change the priority by moving the selected subtree up or down in the list.
  - *Object ID* — Enter an OID not offered in the *Select from List* option.
- **Filter Type** — Indicates whether OID-based informs or traps are sent to trap recipients.
  - *Excluded* — Restricts sending OID traps or informs.
  - *Included* — Sends OID traps or informs.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The SNMP Notification Filter is added to the list, and the device is updated.

## Managing Cisco Discovery Protocol

The *Cisco Discovery Protocol* (CDP) is a Cisco proprietary protocol that enables devices to advertise their existence to other devices by CDP sending out periodic updates to a Multicast address. In addition, CDP allows devices to receive information about other devices on the same LAN or on the remote WAN side. The system supports CDP versions 1 and 2. To enable CDP on the device:

**STEP 1** Click **Monitor & Device Properties > CDP**. The *CDP Page* opens:

### CDP Page

Device ID	Local Interface	Advertise Version	Time to Live	Capabilities	Platform	Port ID
SEP0015C6DC3205	e2	2	160	H P	Cisco IP Phone 7960	Port 1
SEP001F6C7F33C9	e3	2	160	H P	Cisco IP Phone 7945	Port 1
SEP000DE0BF784	e4	2	150	H	Cisco IP Phone 7905	Port 1
SEP001F6C7F37E0	e5	2	155	H P	Cisco IP Phone 7945	Port 1
UC520.atl0.cbeyond.net	e20	2	125	R S I	Cisco UC520-16U-4FX0-K9	FastEthern
00211bf67458	g1	2	170	S I D	ESW-540-24P	g24

The *CDP Page* contains the following fields:

- **CDP Status** — Indicates if CDP is enabled on the device. The possible field values are:
  - *Enable* — Enables CDP on the device. This is the default value.
  - *Disable* — Disables CDP on the device.
- **Voice VLAN** — Indicates the VLAN ID advertised by the device. The Voice VLAN is advertised when a local 802.1Q interface has been configured to send and receive VoIP packets. The field default value is 100.

- **Device ID** — Indicates the device ID TLV which is advertised by neighboring devices.
- **Local Interface** — Indicates the receiving port number.
- **Advertise Version** — Indicates the CDP version advertised by the neighboring device.
- **Time to Live** — Indicates the amount of time in seconds before the neighboring device CDP information is aged out. The field default is 180 seconds.
- **Capabilities** — Indicates the device capabilities advertised by the neighboring devices. The possible field values are:
  - R — Router
  - T — Trans Bridge
  - B — Source Route Bridge
  - S — Switch
  - H — Host
  - I — IGMP
  - r — Repeater
  - P — Phone
  - D — Remote
  - C — CVTA
  - M — Two-port MAC Relay
- **Platform** — Indicates product name and model number of the neighboring device.
- **Port ID** — Indicates the neighboring device's port from which the CDP packet was sent.

**STEP 2** Select *Enable* in the *CDP Status* field to enable the Cisco Discovery Protocol on the device.

**STEP 3** Define a VLAN ID to be advertised by the device in the *Voice VLAN* field.

**STEP 4** Click **Apply**. CDP is enabled, and the device is updated.

To view additional neighboring device CDP information:

**STEP 1** Click **Monitor & Device Properties > CDP**. The *CDP Page* opens

**STEP 2** Click **Details**. The *CDP Neighbor Details Page* opens:

#### CDP Neighbor Details Page

Neighbors Details	
Device ID	00211bfe7458
Advertisement Version	2
IP Address	192.168.10.82
Platform	ESW-540-24P
Capabilities	S I D
Interface	g1
Port ID (outgoing port)	g24
Time To Live	140 sec
Version	1.0.0.16

In addition to the fields in the *CDP Page*, the *CDP Neighbor Details Page* contains the following additional fields:

- **IP Address** — Indicates the address TLV advertised by the neighboring port.
- **Interface** — Indicates the interface type advertised by the neighboring port. The possible field values are:
  - *Ethernet* — Indicates the neighboring interface is an Ethernet port.
  - *Fast Ethernet* — Indicates the neighboring interface is an Fast Ethernet port.
  - *Giga Ethernet* — Indicates the neighboring interface is an Giga Ethernet port.
- **Port ID (outgoing port)** — Indicates the neighboring device's port from which the CDP packet was sent.
- **Version** — Indicates the software version installed on the neighboring device.

# Managing System Files

This section contains information for defining file maintenance and includes both configuration file management as well as device access.

The File Management section contains the following topics:

- Software Upgrade
- Save Configuration
- Copy Configuration File
- Active Image
- DHCP Auto Configuration

The configuration file structure consists of the following configuration files:

- **Startup Configuration File** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted.
- **Running Configuration File** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Backup Configuration File** — Contains a backup copy of the device configuration. The Backup file is generated when the Running Configuration file or the Startup file is copied to the Backup file. The commands copied into the file replaces the existing commands saved in the Backup file. The Backup file contents can be copied to either the Running configuration or the Startup Configuration files.

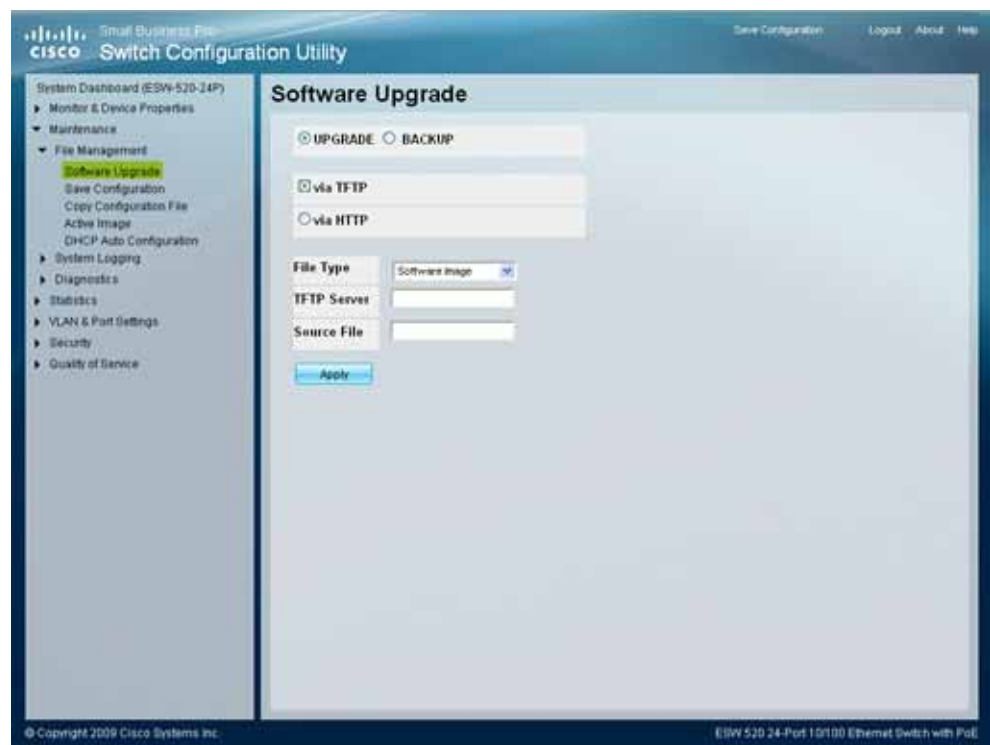
- **Image Files** — Software upgrades are used when a new version file is downloaded.

## Software Upgrade

Firmware files are downloaded as required for upgrading the firmware version or for backing up the system configuration. File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "\_"). The *Software Upgrade Page* contains parameters for downloading system files. To perform a software upgrade:

- STEP 1** Click **Maintenance > File Management > Software Upgrade**. The *Software Upgrade Page* opens:

### Software Upgrade Page



The screenshot shows the Cisco Switch Configuration Utility interface for a Small Business Pro switch. The left sidebar contains a navigation menu with categories like System Dashboard, Monitor & Device Properties, Maintenance, File Management, and System Logging. The 'Software Upgrade' option under File Management is highlighted. The main content area is titled 'Software Upgrade' and contains two radio buttons for 'UPGRADE' (selected) and 'BACKUP'. Below these are two checkboxes for 'via TFTP' (selected) and 'via HTTP'. There are input fields for 'File Type' (set to 'Software Image'), 'TFTP Server', and 'Source File'. An 'Apply' button is at the bottom. The footer includes copyright information and the switch model: 'ESW 520 24-Port 10/100 Ethernet Switch with PoE'.

The *Software Upgrade Page* contains the following fields:

- **UPGRADE** — Specifies that firmware is downloaded for a firmware upgrade.

- **BACKUP** — Specifies that firmware is uploaded for a firmware backup.
- **via TFTP** — Indicates that the upgrade file is found on a TFTP server.
- **via HTTP** — Indicates that the upgrade file is found on a HTTP server.
- **File Type** — Specifies the file type of the downloaded file (for TFTP download only). The possible field values are:
  - *Software Image* — Downloads the Image file.
  - *Boot Code* — Downloads the Boot file.



**NOTE** Boot image upgrade is supported by TFTP protocol, but not supported by HTTP protocol.

- **TFTP Server** — Specifies the TFTP Server IP Address from which files are downloaded.
- **Source File** — Specifies the file to be downloaded. This field is applicable for UPGRADE only.
- **Destination File** — Specifies the file name on the TFTP server where the uploaded file is saved. This field is applicable for BACKUP only.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. Firmware upgrade is defined, and the device is updated.

## Save Configuration

In the *Save Configuration Page*, network administrators can save configuration files on the device.

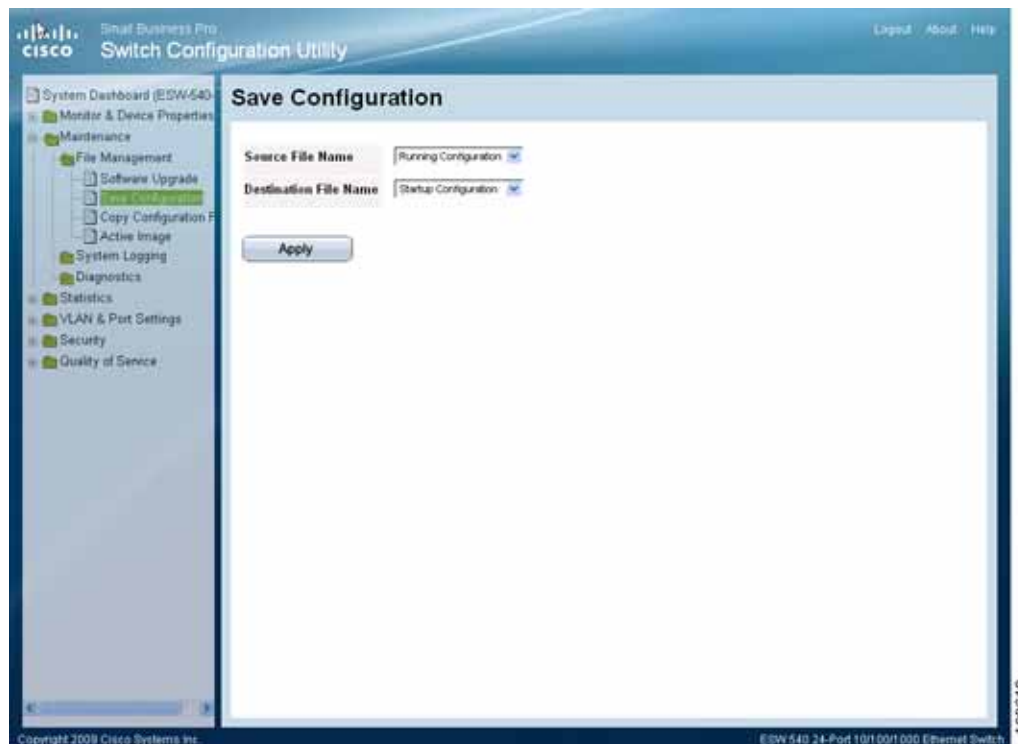
In the *Save Configuration Page*, network administrators can copy configuration files from one device to another.

These steps can be done from the Menu-Based CLI or from the web interface.

- Copy image from TFTP to device
- Change active image on device
- Reboot device

- STEP 1** Click **Maintenance > File Management > Save Configuration**. The *Save Configuration* Page opens:

#### Save Configuration Page



The *Save Configuration* Page contains the following fields:

**Source File Name** — Indicates the device configuration file to copy and the intended usage of the copied file (Running, Startup, or Backup).

**Destination File Name** — Indicates the device configuration file to copy to and the intended usage of the file (Running, Startup, or Backup).

- STEP 2** Define the relevant fields.
- STEP 3** Click **Apply**. The Configuration Files are updated.



**NOTE** Another option to quickly save the Running Configuration to the Startup Configuration is to click Save Configuration at the top of the page. This link is initially grayed out. Once switch configuration changes are made, the link becomes active.



## Copy Configuration

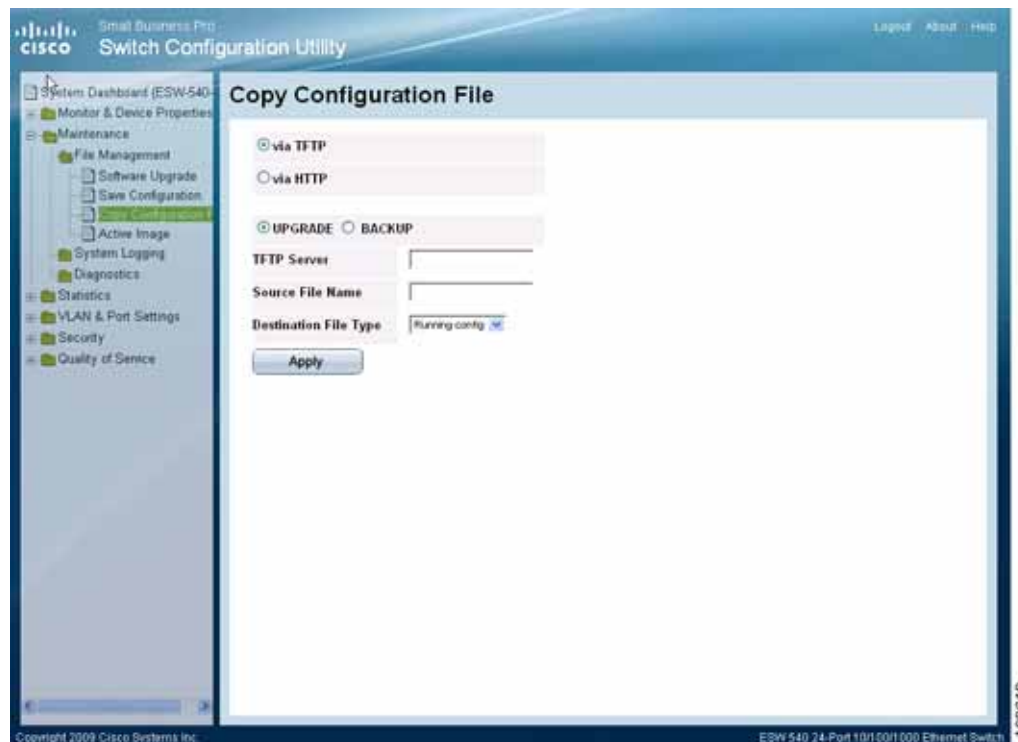
The configuration files control the operation of the switch, and contain the functional settings at the device and the port level. Configuration files are one of the following types:

- **Factory Default** — Contains preset default parameter definitions which are downloaded with a new or upgraded version.
- **Running Configuration** — Contains the parameter definitions currently defined on the device. This includes any configuration changes made since the device was started or rebooted.
- **Starting configuration** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted.
- **Backup configuration** — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.

File names cannot contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "\_").

- STEP 1** Click **Maintenance > File Management > Copy Configuration File**. The *Copy Configuration File Page* opens:

#### Copy Configuration File Page



The *Copy Configuration File Page* contains the following fields:

- **via TFTP** — Download and upload files using TFTP.
- **via HTTP** — Download and upload files using HTTP.

#### Via TFTP

- **UPGRADE** — Specifies that the configuration file is associated with a upgrade.
- **BACKUP** — Specifies that the configuration file contains the system backup configuration.
- **TFTP Server** — Specifies the TFTP Server IP Address for downloading or uploading the file.
- **Source File Name** — Name of the configuration file.

- **Destination File Type** — Specifies the type of configuration file to be created. The possible values are:
  - *Running Config* — Contains the configuration currently valid on the device.
  - *Starting Config* — Contains the configuration which will be valid following system startup or reboot. The Startup configuration is only active after the device is reset.
  - *Backup Config* — Contains a copy of the system configuration for restoration following a shutdown or a fault.

### Via HTTP

Use the *Browse* button to navigate to the file.

- **File Name** — Name of the source configuration file.

**STEP 2** Define the relevant fields and filenames.

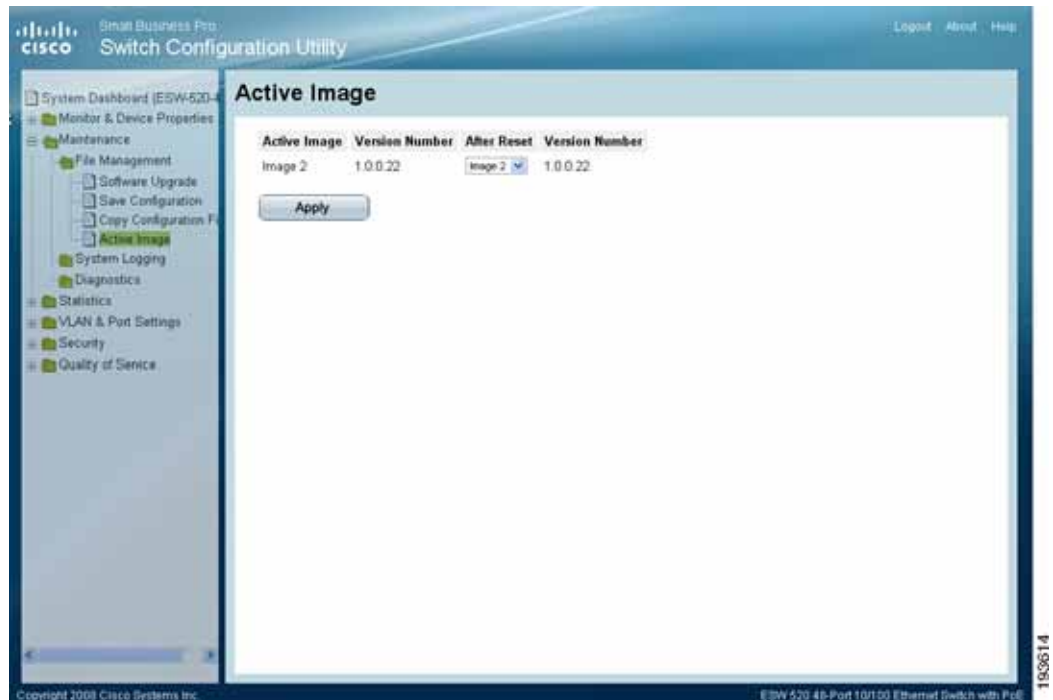
**STEP 3** Click **Apply**. The Copy configuration is defined, and the device is updated.

## Active Image

The *Active Image Page* allows network managers to select the Image files. Images are activated only after the device is reset.

- STEP 1** Click **Maintenance > File Management > Active Image**. The *Active Image Page* opens:

#### Active Image Page



The *Active Image Page* contains the following fields:

- **Active Image** — Indicates the Image file which is currently active on the device.
- **Version Number** — Indicates the image version number currently active on the device.
- **After Reset** — The Image file which is active after the device is reset. The possible field values are:
  - *Image 1* — Activates Image file 1 after the device is reset.
  - *Image 2* — Activates Image file 2 after the device is reset.
- **Version Number** — Indicates the image version number that is active after the device is reset.

- STEP 2** Define the relevant fields.

- STEP 3** Click **Apply**. The active image is defined, and the device is updated.

# DHCP Auto Configuration

Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network.

The *DHCP Auto Configuration Page* allows network managers to change the configuration file and store it on the TFTP server in their network. This configuration file is downloaded automatically to all the switches in the network on which DHCP Auto Configuration is enabled.

The *DHCP Auto Configuration Page* contains the following fields:

- **Auto Configuration Via DHCP**— Indicates whether or not DHCP Auto Configuration is enabled in the device.
  - *Enable* — Enables DHCP Auto Configuration on the device. This is the default value.
  - *Disable* — Disables DHCP Auto Configuration on the device.
- **Renew DHCP Address** — When enabled specifies that the device will connect to the DHCP Server and renew the IP Address after clicking **Apply**.
  - *Checked* — Enables automatic renewal of IP Address on the device.
  - *Unchecked* — Disables automatic renewal of IP Address on the device. This is the default value.
- **Force Auto Configuration From DHCP** — When enabled specifies that the Auto Configuration process will take place when the switch is connected to the DHCP Server to renew its IP Address.
  - *Checked* — Enables auto configuration when the switch is connected to the DHCP Server.
  - *Unchecked* — Disables auto configuration when the switch is connected to the DHCP Server.

# Managing Power-over-Ethernet Devices

Power-over-Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power-over-Ethernet removes the necessity of placing network devices next to power sources.

Power-over-Ethernet can be used in the following applications:

- IP Phones
- Wireless Access Points
- IP Gateways
- Audio and Video Remote Monitoring

Powered Devices are devices which receive power from the device power supplies, for example IP phones. Powered Devices are connected to the device via Ethernet ports. Guard Band protects the device from exceeding the maximum power level. For example, if 400W is maximum power level, and the Guard Band is 20W, if the total system power consumption exceeds 380W no additional PoE components can be added. The accumulated PoE components power consumption is rounded down for display purposes, therefore remove value after decimal point.

This section contains the following section:

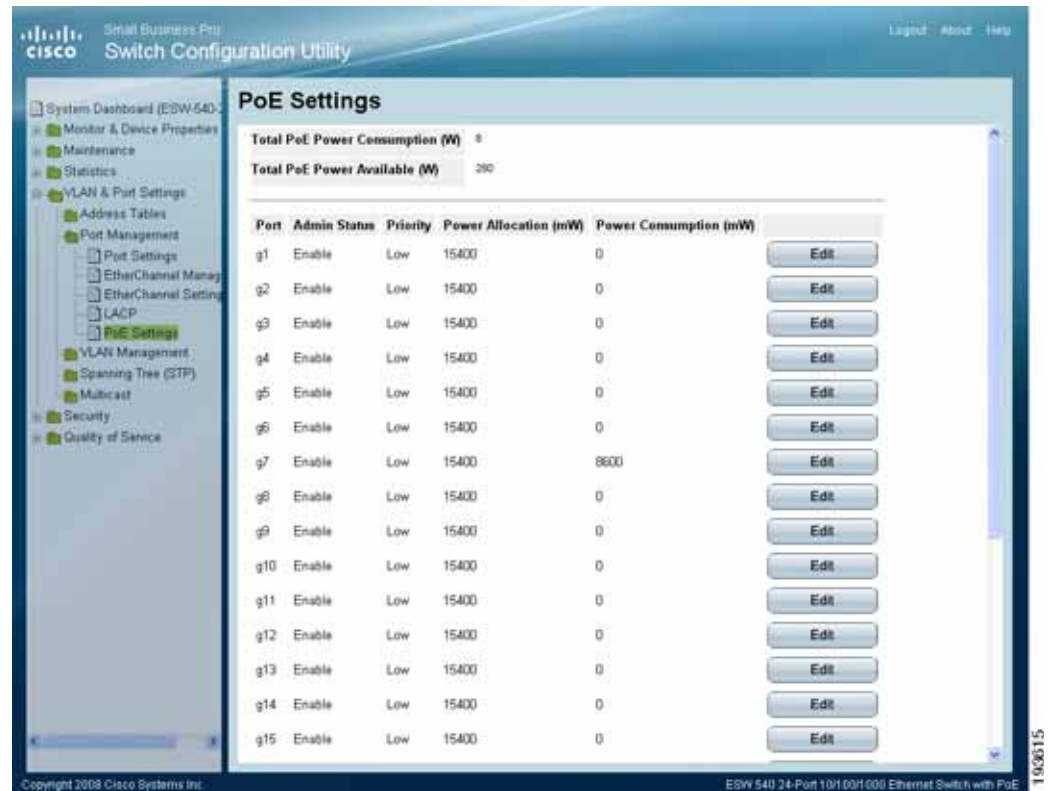
- Defining PoE Settings

## Defining PoE Settings

The *PoE Settings Page* contains system PoE information for enabling PoE on the device, monitoring the current power usage, and enabling PoE traps. To configure PoE Settings:

**STEP 1** Click **VLAN & Port Settings > Port Management > PoE Settings**. The *PoE Settings* Page opens:

#### PoE Settings Page



The *PoE Settings* Page displays the currently configured PoE ports and contains the following information:

- **Total PoE Power Consumption (W)** — Displays the total amount of power consumed by PoE ports.
- **Total PoE Power Available (W)** — Displays the total amount of power available to PoE ports.
- **Port** — Displays the selected port number.
- **Admin Status** — Indicates whether PoE is enabled or disabled on the port. The possible values are:
  - *Enable* — Enables PoE on the port. This is the default setting.
  - *Disable* — Disables PoE on the port.

- **Priority** — Indicates the PoE port priority. The possible values are: *Critical*, *High* and *Low*. The default is *Low*.
- **Power Allocation (mW)** — Indicates the power in milliwatts allocated to the port. The range is 0 - 15,400.
- **Power Consumption (mW)** — Indicates the amount of power in milliwatts assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the classification information used.

**STEP 2** Click the **Edit** button. The *Edit PoE Settings Page* opens:

#### Edit PoE Settings Page

The screenshot shows the 'Edit PoE Settings' page for port 'e1'. The settings are as follows:

Field	Value
Port	e1
Enable PoE	<input checked="" type="checkbox"/>
Power Priority Level	Low
Power Allocation	15400
Power Consumption	5300
Overload Counter	0
Short Counter	0
Denied Counter	0
Absent Counter	6
Invalid Signature Counter	0

An 'Apply' button is located at the bottom right of the form.

The Edit PoE Settings Page contains the following fields:

- **Port** — Indicates the specific interface for which PoE parameters are defined, and assigned to the powered interface connected to the selected port.
- **Enable PoE** — Enables or disables PoE on the port. The possible values are:
  - *Checked* — Enables PoE on the port. This is the default setting.
  - *Unchecked* — Disables PoE on the port.
- **Power Priority Level** — Determines the port priority if the power supply is low. The field default is low. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 3 is prioritized as low, port 1 is prioritized to receive power, and port 3 may be denied power. The possible field values are:



- *Low* — Defines the PoE priority level as low.
  - *High* — Defines the PoE priority level as high.
  - *Critical* — Defines the PoE priority level as Critical. This is the highest PoE priority level.
- **Power Allocation** — Indicates the power in milliwatts allocated to the port. The range is 0 - 15,400.
- **Power Consumption** — Indicates the amount of power in milliwatts assigned to the powered device connected to the selected interface. Devices are classified by the powered device, and the classification information used. The possible power ranges and their corresponding classes are:
  - *440 to 12950* — (Powered device Class 0) Indicates that the port is assigned a power consumption level of 0.44 to 12.95 watts. This is the default.
  - *440 to 3840* — (Powered device Class 1) Indicates that the port is assigned a power consumption level of 0.44 to 3.84 watts.
  - *3840 to 6490* — (Powered device Class 2) Indicates that the port is assigned a power consumption level of 3.84 to 6.49 watts.
  - *6490 to 12950* — (Powered device Class 3) Indicates that the port is assigned a power consumption level of 6.49 to 12.95 watts.
- **Overload Counter** — Indicates the total power overload occurrences.
- **Short Counter** — Indicates the total power shortage occurrences.
- **Denied Counter** — Indicates times the powered device was denied power.
- **Absent Counter** — Indicates the times the power supply was stopped to the powered device because the powered device was no longer detected.
- **Invalid Signature Counter** — Indicate the times an invalid signature was received. Signatures are the means by which the powered device identifies itself to the PSE. Signature are generated during powered device detection, classification, or maintenance.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The PoE Settings are defined, and the device is updated.

# Managing System Logs

The System Logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors or informational messages.

Event messages have a unique format, as per the SYSLOG protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event logging.

This section contains the following pages:

- [Enabling System Logs](#)
- [Viewing the Device Memory Logs](#)
- [Viewing the System Flash Logs](#)
- [Viewing Remote Logs](#)

## Enabling System Logs

In the *System Messages Settings Page*, define the levels of event severity that are recorded to the system event logs.

The event severity levels are listed on this page in descending order from the highest severity to the lowest. When a severity level is selected to appear in a log, all higher severity events will automatically be selected to appear in the log. Conversely, when a security level is not selected, no lower severity events will appear in the log.

For example, if Warning is selected, all severity levels higher and including Warning will appear in the log. Additionally, no events with a lower severity level than Warning will be listed.

To define Log Global Parameters:

- STEP 1** Click **Maintenance > System Logging > System Messages Settings**. The *System Messages Settings Page* opens.

#### System Messages Settings Page



The *System Messages Settings Page* contains the following fields:

- **Enable Logging** — Indicates if message logging is enabled globally in the device.
- **Severity** — The following are the available severity levels:
  - *Emergency* — The system is not functioning.
  - *Alert* — The system needs immediate attention.
  - *Critical* — The system is in a critical state.
  - *Error* — A system error has occurred.
  - *Warning* — A system warning has occurred.
  - *Notice* — The system is functioning properly, but system notice has occurred.
  - *Informational* — Provides device information.

## Managing System Logs

### Viewing the Device Memory Logs

- *Debug* — Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.
- **Memory Logs** — The selected Severity types will appear in chronological order in all system logs that are saved in RAM (Cache). After restart, these logs are deleted.
- **Flash Logs** — The selected Severity types will be sent to the Logging file kept in FLASH memory. After restart, this log is not deleted.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The global log parameters are set, and the device is updated.

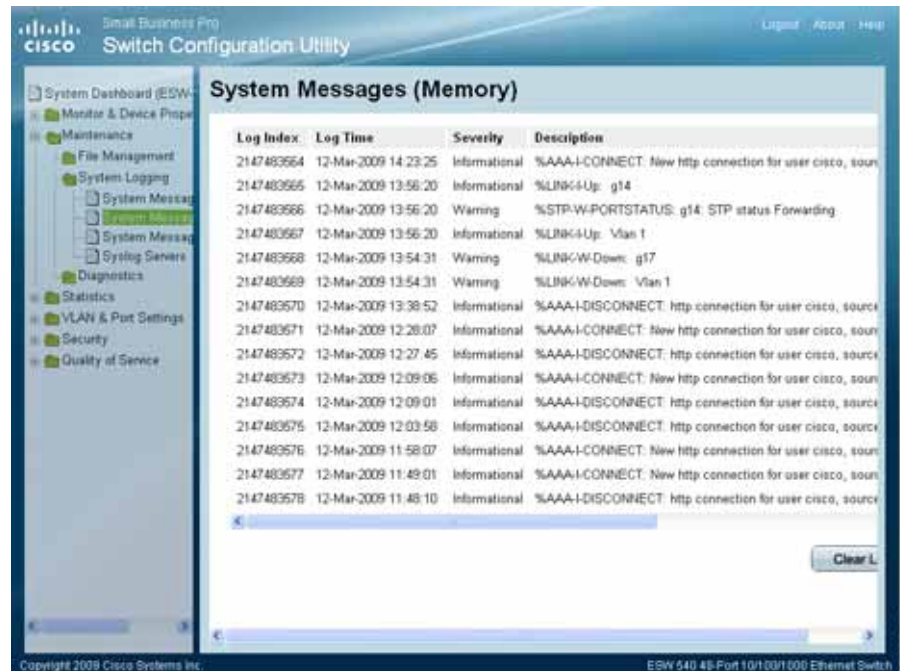
## Viewing the Device Memory Logs

The System Messages (Memory) Page contains all system log entries in chronological order that are saved in RAM (Cache). After restart, these log entries are deleted.

To open the *System Messages (Memory) Page*:

- STEP 1** Click **Maintenance > System Logging > System Messages (Memory)**. The *System Messages (Memory) Page* opens.

#### System Messages (Memory) Page



The System Messages (Memory) Page contains the following fields:

- **Log Index** — Displays the log entry number.
- **Log Time** — Displays the time at which the log entry was generated.
- **Severity** — Displays the event severity.
- **Description** — Displays the log message text.

#### Clearing Message Logs

Message Logs can be cleared from the *System Messages (Memory) Page*. To clear the *System Messages (Memory) Page*:

- STEP 1** Click **Maintenance > System Logging > System Messages (Memory)**. The *System Messages (Memory) Page* opens.
- STEP 2** Click the **Clear Logs** button. The message logs are cleared.

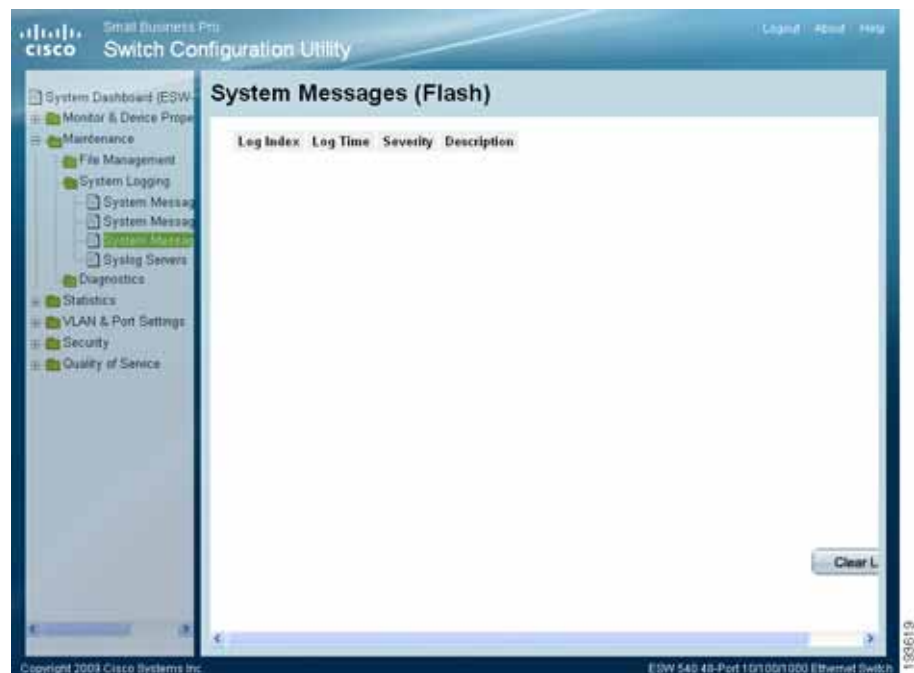
## Viewing the System Flash Logs

The *System Messages (Flash)* Page contains information about log entries saved to the Log File in FLASH, including the time the log was generated, the event severity, and a description of the log message. The Message Log is available after reboot.

To view the Flash Logs:

- STEP 1** Click **Maintenance > System Logging > System Messages (Flash)**. The *System Messages (Flash)* Page opens:

### System Messages (Flash) Page



The *System Messages (Flash)* Page contains the following fields:

- **Log Index** — Displays the log entry number.
- **Log Time** — Displays the time at which the log entry was generated.
- **Severity** — Displays the event severity.
- **Description** — Displays the log message text.

## Clearing Flash Logs

Flash Logs can be cleared from the *System Messages (Flash) Page*. To clear the *System Messages (Flash) Page*:

- STEP 1** Click **Maintenance > System Logging > System Messages (Flash)**. The *System Messages (Flash) Page* opens.
- STEP 2** Click **Clear Logs**. The message logs are cleared.

## Remote Log Servers

The *Syslog Servers Page* contains information for configuring the Remote Log Servers. New log servers and the minimum severity level of events sent to them may be added.

- STEP 1** Click **Maintenance > System Logging > Syslog Servers**. The *Syslog Servers Page* opens:

### Syslog Servers Page



The *Syslog Servers Page* contains the following fields:

- **Server** — Specifies the server IP address to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 - Local 7**.
- **Description** — Provides a user-defined server description.
- **Minimum Severity** — Indicates the minimum severity level for logs that are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.

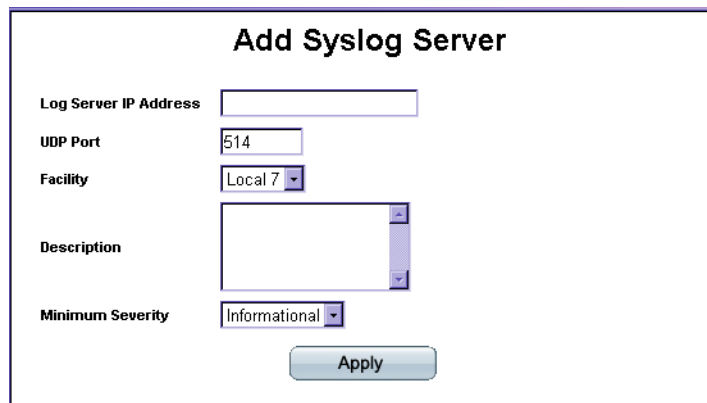
The following are the available log severity levels:

- *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
- *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- *Error* — A device error has occurred, for example, if a single port is offline.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- *Notice* — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

**STEP 2** Click the **Add** button. The *Add Syslog Server Page* opens:



#### Add Syslog Server Page



The screenshot shows a web form titled "Add Syslog Server". It contains the following fields:

- Log Server IP Address**: A text input field.
- UDP Port**: A text input field containing the value "514".
- Facility**: A dropdown menu with "Local 7" selected.
- Description**: A text area for a user-defined description.
- Minimum Severity**: A dropdown menu with "Informational" selected.
- Apply**: A button at the bottom right of the form.

The *Add Syslog Server Page* contains fields for defining new Remote Log Servers.

The *Add Syslog Server Page* contains the following fields:

- **Log Server IP Address** — Specifies the server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 - Local 7**.
- **Description** — Provides a user-defined server description.
- **Minimum Severity** — Indicates the minimum severity level of logs that are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.

The following are the available log severity levels:

- *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.

- *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- *Error* — A device error has occurred, for example, if a single port is offline.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- *Notice* — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

**STEP 3** Define the relevant fields.

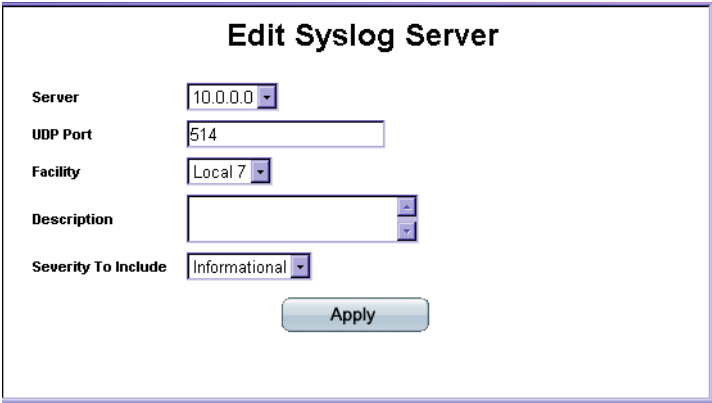
**STEP 4** Click **Apply**. The *Add Syslog Server Page* closes, the syslog server is added, and the device is updated.

## Modifying Syslog Server Settings

**STEP 1** Click **Maintenance > System Logging > Syslog Servers**. The *Syslog Servers Page* opens:

**STEP 2** Click the **Edit** button. The *Edit Syslog Server Page* opens:

### Edit Syslog Server Page



The screenshot shows the 'Edit Syslog Server' form. It contains the following fields and controls:

- Server**: A dropdown menu with '10.0.0.0' selected.
- UDP Port**: A text input field containing '514'.
- Facility**: A dropdown menu with 'Local 7' selected.
- Description**: A text input field with a small expand/collapse icon on the right.
- Severity To Include**: A dropdown menu with 'Informational' selected.
- Apply**: A button located at the bottom right of the form.

The *Edit Syslog Server Page* contains fields for modifying Remote Log Server settings.

The *Edit Syslog Server Page* contains the following fields:

- **Server** — Specifies the name of the Remote Log Server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are **Local 0 - Local 7**.
- **Description** — Provides a user-defined server description.
- **Severity to Include** — Indicates the minimum severity level for logs that are sent to the server. For example, if Notice is selected, all logs from a Notice severity and higher are sent to the remote server.

The following are the available log severity levels:

- *Emergency* — The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- *Alert* — The second highest warning level. An alert log is saved, if there is a serious device malfunction; for example, all device features are down.
- *Critical* — The third highest warning level. A critical log is saved if a critical device malfunction occurs; for example, two device ports are not functioning, while the rest of the device ports remain functional.
- *Error* — A device error has occurred, for example, if a single port is offline.
- *Warning* — The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- *Notice* — The system is functioning properly, but system notice has occurred.
- *Informational* — Provides device information.
- *Debug* — Provides debugging messages.

#### **STEP 3** Define the relevant fields.

## Managing System Logs

### Remote Log Servers

---

**STEP 4** Click **Apply**. The Syslog Server settings are modified, and the device is updated.

# Viewing Statistics

This section describes device statistics for RMON, interfaces, GVRP, EAP, and Etherlike statistics. This section contains the following topics:

- Viewing Ethernet Statistics
- Managing RMON Statistics
- Managing QoS Statistics

## Viewing Ethernet Statistics

The Ethernet section contains the following pages:

- Defining Interface Statistics
- Viewing Etherlike Statistics
- Viewing GVRP Statistics
- Viewing EAP Statistics

### Defining Interface Statistics

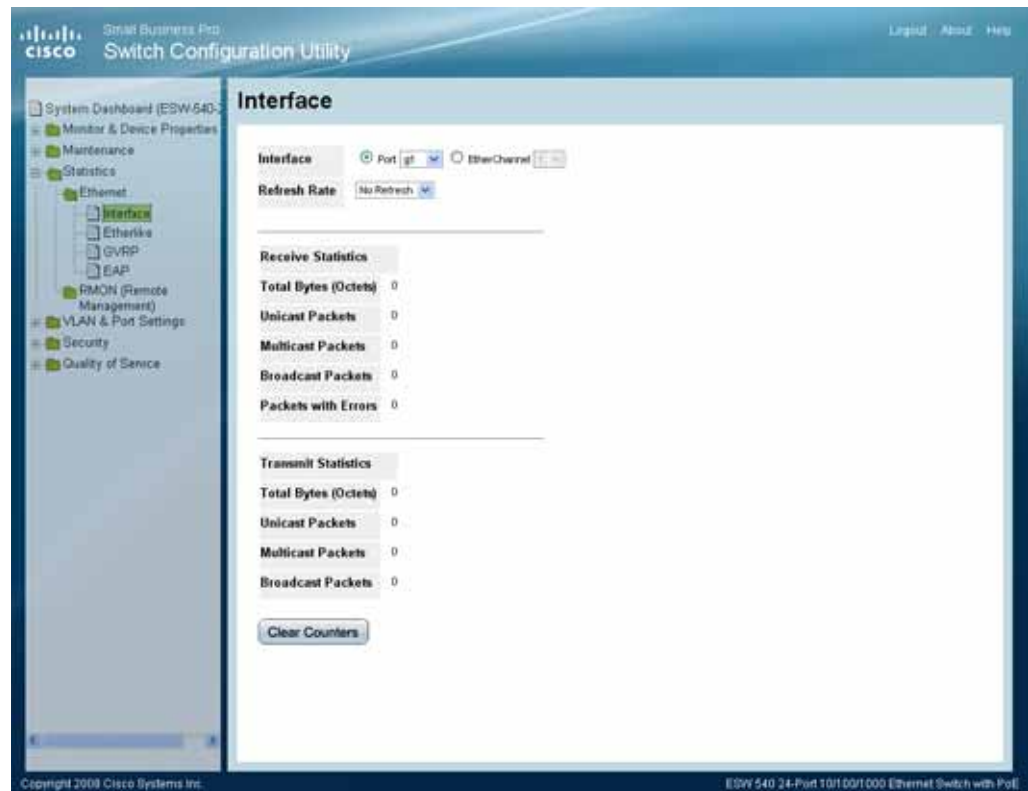
The *Interface Statistics Page* contains statistics for both received and transmitted packets. The *Interface Statistics Page* is divided into three areas, General Information, Receive Statistics and Transmit Statistics.

## Viewing Statistics

### Viewing Ethernet Statistics

**STEP 1** Click **Statistics > Ethernet > Interface**. The *Interface Statistics Page* opens:

#### Interface Statistics Page



The *Interface Statistics Page* contains the following fields:

- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
  - *Port* — Defines the specific port for which Ethernet statistics are displayed.
  - *EtherChannel* — Defines the specific EtherChannel for which Ethernet statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the Ethernet statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the Ethernet statistics are refreshed every 30 seconds.

## Viewing Statistics

### Viewing Ethernet Statistics

- *60 Sec* — Indicates that the Ethernet statistics are refreshed every 60 seconds.
- *No Refresh* — Indicates that the Ethernet statistics are not refreshed.

The Receive Statistics area contains the following fields:

- **Total Bytes (octets)** — Displays the number of octets received on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Unicast Packets** — Displays the number of good Unicast packets received on the interface since the page was last refreshed.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the page was last refreshed.
- **Broadcast Packets** — Displays the number of good broadcast packets received on the interface since the page was last refreshed.
- **Packets with Errors** — Displays the number of packets with errors.

The Transmit Statistics area contains the following fields:

- **Total Bytes (octets)** — Displays the number of octets transmitted on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Unicast Packets** — Displays the number of good Unicast packets transmitted on the interface since the page was last refreshed.
- **Multicast Packets** — Displays the number of good Multicast packets transmitted on the interface since the page was last refreshed.
- **Broadcast Packets** — Displays the number of good broadcast packets transmitted on the interface since the page was last refreshed.

### Resetting Interface Statistics Counters

**STEP 1** Click **Statistics > Ethernet > Interface**. The *Ethernet Interface Page* opens:

**STEP 2** Click the **Clear Counters** button. The interface statistics counters are cleared.

### Viewing Etherlike Statistics

The *Etherlike Page* contains interface statistics.

## Viewing Statistics

### Viewing Ethernet Statistics

To view Etherlike Statistics:

**STEP 1** Click **Statistics > Ethernet > Etherlike**. The *Etherlike Page* opens:

#### Etherlike Page



The *Etherlike Page* contains Ethernet-like interface statistics. The *Etherlike Page* contains the following fields:

- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
  - *Port* — Defines the specific port for which Etherlike statistics are displayed.
  - *EtherChannel* — Defines the specific EtherChannel for which Etherlike statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the Etherlike statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the Etherlike statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the Etherlike statistics are refreshed every 30 seconds.



## Viewing Statistics

### Viewing Ethernet Statistics

- *60 Sec* — Indicates that the Etherlike statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the Etherlike statistics are not refreshed.
- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.
- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
- **Excessive Collisions** — Displays the number of excessive collision frames received on the selected interface. (Available on non-gigabit switches only)
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the page was last refreshed.
- **Internal MAC Receive Errors** — Displays the number of internal MAC received errors on the selected interface
- **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
- **Transmitted Pause Frames** — Displays the number of paused frames transmitted from the selected interface.

### Resetting Etherlike Statistics Counters

- 
- STEP 1** Click **Statistics > Ethernet > Etherlike**. The *Etherlike Page* opens:
- STEP 2** Click the **Clear Counters** button. The interface statistics counters are cleared.

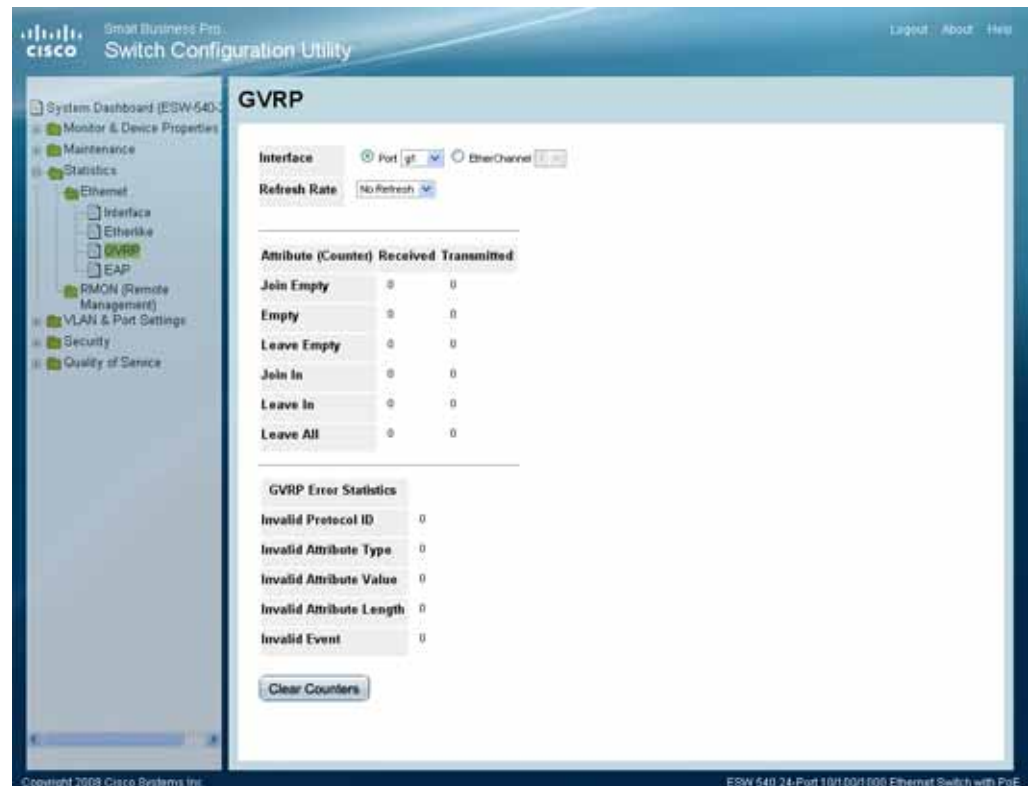
### Viewing GVRP Statistics

The *GVRP Page* contains statistics for GVRP communication on the device.

To view GVRP statistics:

**STEP 1** Click **Statistics > Ethernet > GVRP**. The *GVRP Page* opens:

#### GVRP Page



The *GVRP Page* is divided into two areas, GVRP Statistics Table and GVRP Error Statistics Table.

The following fields are relevant for both tables:

- **Interface** — Indicates the interface for which statistics are displayed. The possible field values are:
  - *Port* — Defines the specific port for which GVRP statistics are displayed.
  - *EtherChannel* — Defines the specific EtherChannel for which GVRP statistics are displayed.
- **Refresh Rate** — Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the GVRP statistics are refreshed every 15 seconds.

## Viewing Statistics

### Viewing Ethernet Statistics

- *30 Sec* — Indicates that the GVRP statistics are refreshed every 30 seconds.
- *60 Sec* — Indicates that the GVRP statistics are refreshed every 60 seconds.
- *No Refresh* — Indicates that the GVRP statistics are not refreshed.

The GVRP Received Transmitted Table contains the following fields:

- **Join Empty** — Displays the device GVRP Join Empty statistics.
- **Empty** — Displays the device GVRP Empty statistics.
- **Leave Empty** — Displays the device GVRP Leave Empty statistics.
- **Join In** — Displays the device GVRP Join In statistics.
- **Leave In** — Displays the device GVRP Leave in statistics.
- **Leave All** — Displays the device GVRP Leave all statistics.

The GVRP Error Statistics Table contains the following fields:

- **Invalid Protocol ID** — Displays the device GVRP Invalid Protocol ID statistics.
- **Invalid Attribute Type** — Displays the device GVRP Invalid Attribute ID statistics.
- **Invalid Attribute Value** — Displays the device GVRP Invalid Attribute Value statistics.
- **Invalid Attribute Length** — Displays the device GVRP Invalid Attribute Length statistics.
- **Invalid Event** — Displays the device GVRP Invalid Events statistics.

### Resetting GVRP Statistics Counters

**STEP 1** Click **Statistics > Ethernet > GVRP**. The *GVRP Page* opens.

**STEP 2** Click **Clear Counters**. The GVRP statistics counters are cleared.

## Viewing EAP Statistics

The *EAP Page* contains information about EAP packets received on a specific port.

## Viewing Statistics

### Viewing Ethernet Statistics

To view the EAP Statistics:

**STEP 1** Click **Statistics > Ethernet > EAP**. The *EAP Page* opens:

#### EAP Page



The EAP Page contains the following fields:

- **Port** — Indicates the port which is polled for statistics.
- **Refresh Rate** — Defines the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
  - *15 Sec* — Indicates that the EAP statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the EAP statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the EAP statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the EAP statistics are not refreshed.
- **Frames Received** — Indicates the number of valid EAPOL frames received on the port.

- **Frames Transmitted** — Indicates the number of EAPOL frames transmitted via the port.
- **Start Frames Received** — Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Received** — Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Received** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Received** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Request ID Frames Transmitted** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmitted** — Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Received** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Length Error Frames Received** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** — Indicates the source MAC address attached to the most recently received EAPOL frame.

## Managing RMON Statistics

The RMON section contains the following pages:

- Viewing RMON Statistics
- Configuring RMON History
- Defining RMON Events Control
- Defining RMON Alarms

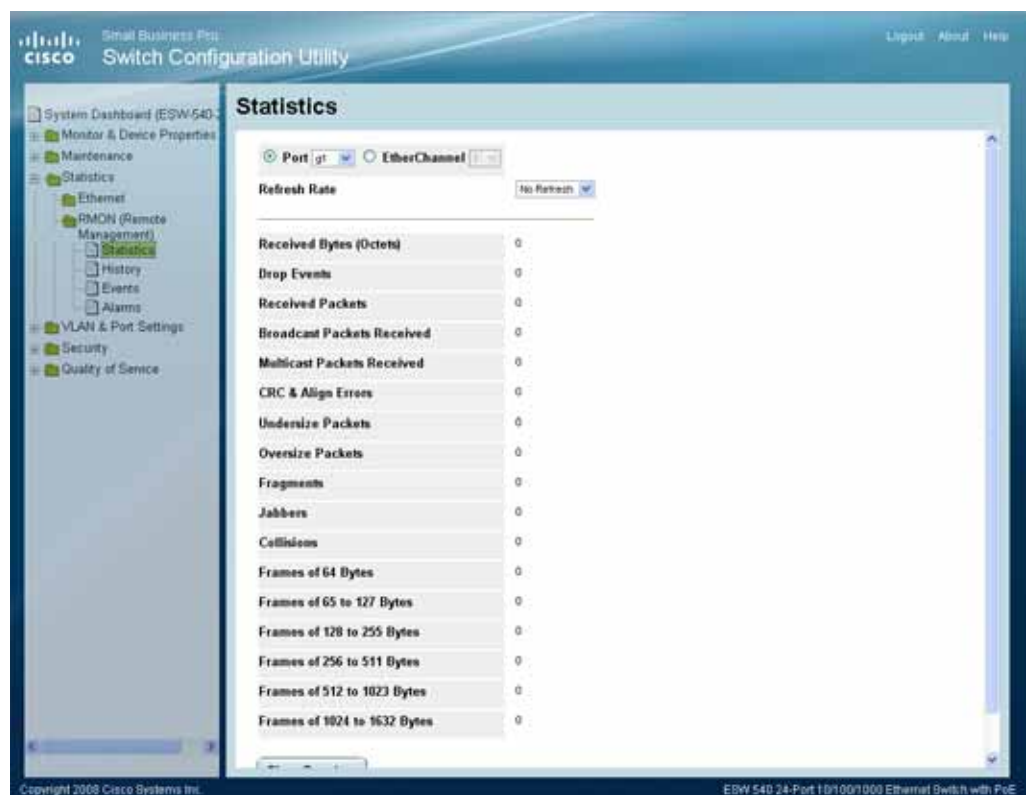
## Viewing RMON Statistics

The *RMON Statistics Page* contains fields for viewing information about device utilization and errors that occurred on the device.

To view the RMON statistics:

- STEP 1** Click **Statistics > RMON (Remote Management) > Statistics**. The *RMON Statistics Page* opens:

### RMON Statistics Page



The *RMON Statistics Page* contains the following fields:

- **Port** — Defines the specific port for which RMON statistics are displayed.
- **EtherChannel** — Defines the specific EtherChannel for which RMON statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:

- *15 Sec* — Indicates that the RMON statistics are refreshed every 15 seconds.
  - *30 Sec* — Indicates that the RMON statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the RMON statistics are refreshed every 60 seconds.
  - *No Refresh* — Indicates that the RMON statistics are not refreshed.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Drop Events** — Displays the number packets that were dropped.
- **Received Packets** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the page was last refreshed.
- **Broadcast Packets Received** — Displays the number of good broadcast packets received on the interface since the page was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the page was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the page was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the page was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the page was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the page was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.

- **Collisions** — Displays the number of collisions received on the interface since the page was last refreshed.
- **Frames of xx Bytes** — Number of frames containing the specified number of bytes that were received on the interface since the page was last refreshed.

**STEP 2** Select either *Port* or *EtherChannel*. The RMON statistics are displayed.

## Resetting RMON Statistics Counters

**STEP 1** Click **Statistics > RMON (Remote Management) > Statistics**. The *RMON Statistics Page* opens:

**STEP 2** Click the **Clear Counters** button. The RMON statistics counters are cleared.

## Configuring RMON History

This section contains the following topics:

- Defining RMON History Control
- Viewing the RMON History Table

### Defining RMON History Control

The *RMON History Control Page* contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

To view RMON history information:

1. Click **Statistics > RMON (Remote Management) > History**. The *RMON History Control Page* opens.



#### RMON History Control Page

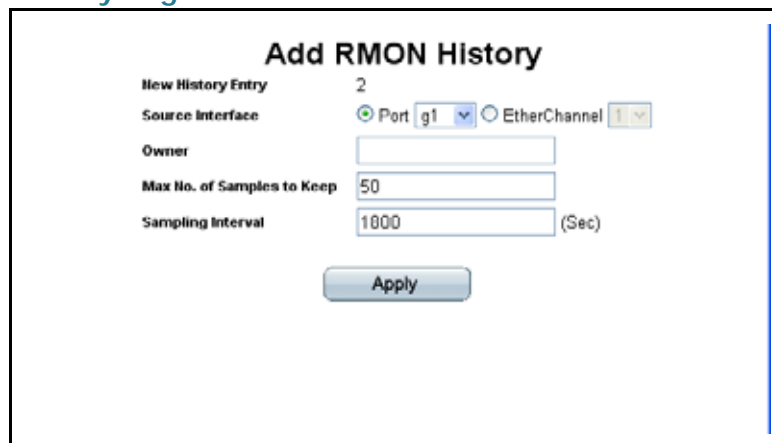


The *RMON History Control Page* contains the following fields:

- **History Entry No.** — Number automatically assigned to the table entry number.
- **Source Interface** — Displays the interface (port or EtherChannel) from which the history samples were taken. The possible field values are:
  - *Port* — Specifies the port from which the RMON information was taken.
  - *EtherChannel* — Specifies the EtherChannel from which the RMON information was taken.
- **Sampling Interval** — Indicates the time in seconds that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- **Sampling Requested** — Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- **Current Number of Samples** — Displays the current number of samples taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.

**STEP 3** Click the **Add** button. The *Add RMON History Page* opens:

#### Add RMON History Page



The screenshot shows the 'Add RMON History' configuration page. It contains the following fields and controls:

- New History Entry:** A text field containing the value '2'.
- Source Interface:** A group box containing two radio buttons. The 'Port' radio button is selected, and its dropdown menu shows 'g1'. The 'EtherChannel' radio button is unselected, and its dropdown menu shows '1'.
- Owner:** An empty text field.
- Max No. of Samples to Keep:** A text field containing the value '50'.
- Sampling Interval:** A text field containing the value '1000', followed by '(Sec)'.
- Apply:** A button at the bottom center of the form.

The *Add RMON History Page* contains the following fields:

- **New History Entry** — Number automatically assigned to the table entry number.
- **Source Interface** — Select the interface (port or EtherChannel) from which the history samples will be taken. The possible field values are:
  - *Ports* — Specifies the port from which the RMON information is taken.
  - *EtherChannel* — Specifies the EtherChannel from which the RMON information is taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Max No. of Samples to Keep** — Indicates the number of samples to save.
- **Sampling Interval** — Indicates the time in seconds that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

**STEP 4** Define the relevant fields.

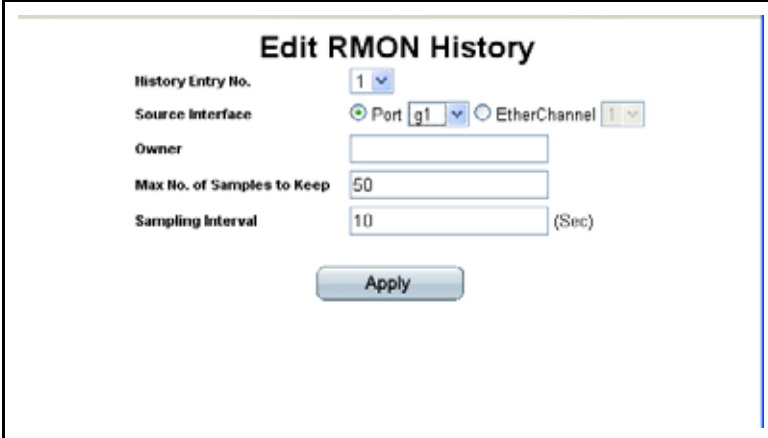
**STEP 5** Click **Apply**. The entry is added to the *RMON History Control Page*, and the device is updated.

#### Modifying RMON History Settings

**STEP 1** Click **Statistics > RMON (Remote Management) > History**. The *RMON History Control Page* opens.

**STEP 2** Click the **Edit** button. The *Edit RMON History Page* opens:

#### Edit RMON History Page

The screenshot shows a web-based configuration interface titled "Edit RMON History". It contains several fields: "History Entry No." with a dropdown menu showing "1"; "Source Interface" with radio buttons for "Port" (selected) and "EtherChannel", and a dropdown for "g1" next to "Port"; "Owner" with a text input field; "Max No. of Samples to Keep" with a text input field showing "50"; and "Sampling Interval" with a text input field showing "10" and a "(Sec)" label. An "Apply" button is located at the bottom center of the form.

The *Edit RMON History Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Source Interface** — Displays the interface (port or EtherChannel) from which the history samples are taken. The possible field values are:
  - *Port* — Specifies the port from which the RMON information is taken.
  - *EtherChannel* — Specifies the EtherChannel from which the RMON information is taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Max No. of Samples to Keep** — Indicates the number of samples to save.
- **Sampling Interval** — Indicates the time in seconds that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The history control settings are modified, and the device is updated.

#### Viewing the RMON History Table

The *RMON History Table Page* contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

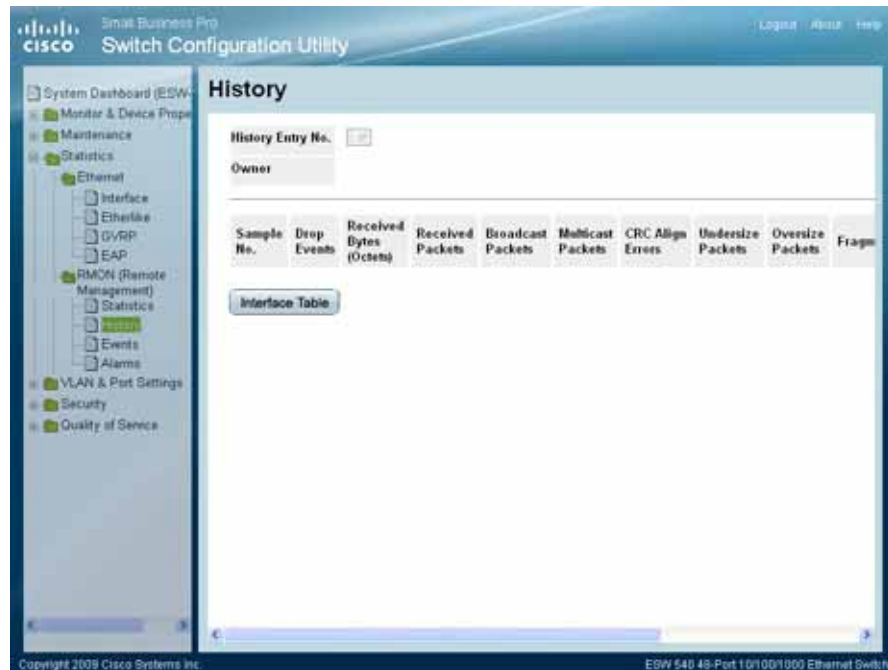
## Viewing Statistics

### Configuring RMON History

**STEP 1** Click **Statistics > RMON (Remote Management) > History**. The *RMON History Control Page* opens:

**STEP 2** Click the **History Table** button. The *RMON History Table Page* opens:

#### RMON History Table Page



The *RMON History Table Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample No.** — Indicates the sample number from which the statistics were taken.
- **Drop Events** — Indicates the number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number dropped packets, but rather the number of times dropped packets were detected.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the page was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.

- **Received Packets** — Displays the number of packets received on the interface since the page was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the page was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the page was last refreshed.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the page was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the page was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the page was last refreshed.
- **Fragments** — Displays the number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the page was last refreshed.
- **Jabbers** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the page was last refreshed.
- **Utilization** — Displays the percentage of the interface utilized.

## Defining RMON Events Control

The *RMON Events Page* contains fields for defining RMON events.

To view RMON events:

- STEP 1** Click **Statistics > RMON (Remote Management) > Events**. The *RMON Events Page* opens:

#### RMON Events Page



The *RMON Events Page* contains the following fields:

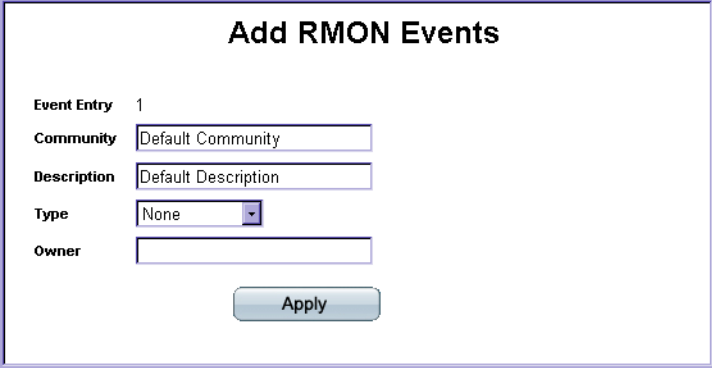
- **Event Entry** — Displays the event index number.
- **Community** — Displays the SNMP community string.
- **Description** — Displays the event description.
- **Type** — Describes the event type. Possible values are:
  - *None* — No action occurs.
  - *Log* — The device adds a log entry.
  - *Trap* — The device sends a trap.
  - *Log and Trap* — The device adds a log entry and sends a trap.
- **Time** — Displays the date and time that the event occurred.
- **Owner** — Displays the device or user that defined the event.

The **Add** button adds the configured RMON event to the Event Table.

The **Delete** button deletes the selected RMON event.

**STEP 2** Click the **Add** button. The *Add RMON Events Page* opens:

### Add RMON Events Page



The screenshot shows a web form titled "Add RMON Events". It contains the following fields and controls:

- Event Entry**: A text field containing the value "1".
- Community**: A text field containing the value "Default Community".
- Description**: A text field containing the value "Default Description".
- Type**: A dropdown menu with "None" selected.
- Owner**: An empty text field.
- Apply**: A button located at the bottom right of the form.

The *Add RMON Events Page* contains the following fields:

- **Event Entry** — Indicates the event entry index number.
- **Community** — Displays the SNMP community string.
- **Description** — Displays a user-defined event description.
- **Type** — Describes the event type. Possible values are:
  - *None* — No action occurs.
  - *Log* — The device adds a log entry.
  - *Trap* — The device sends a trap.
  - *Log and Trap* — The device adds a log entry and sends a trap.
- **Owner** — Displays the device or user that defined the event.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The RMON event is added, and the device is updated.

### Modifying RMON Event Log Settings

**STEP 1** Click **Statistics > RMON (Remote Management) > Events**. The *RMON Events Page* opens:

**STEP 2** Click **Edit**. The *Edit RMON Events Page* opens:

## Edit RMON Events Page

The screenshot shows a web interface titled "Edit RMON Events". It contains several input fields: "Event Entry No." with a dropdown menu showing "1", "Community" with a text box containing "Default Community", "Description" with a text box containing "Default Description", "Type" with a dropdown menu showing "Log and Trap", and "Owner" with an empty text box. An "Apply" button is located at the bottom right of the form.

The *Edit RMON Events Page* contains the following fields:

- **Entry Event No.** — Displays the event entry index number.
- **Community** — Displays the SNMP community string.
- **Description** — Displays the user-defined event description.
- **Type** — Describes the event type. Possible values are:
  - *None* — No action occurs.
  - *Log* — The device adds a log entry.
  - *Trap* — The device sends a trap.
  - *Log and Trap* — The device adds a log entry and sends a trap.
- **Owner** — Displays the device or user that defined the event.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The event control settings are modified, and the device is updated.

## Viewing the RMON Events Logs

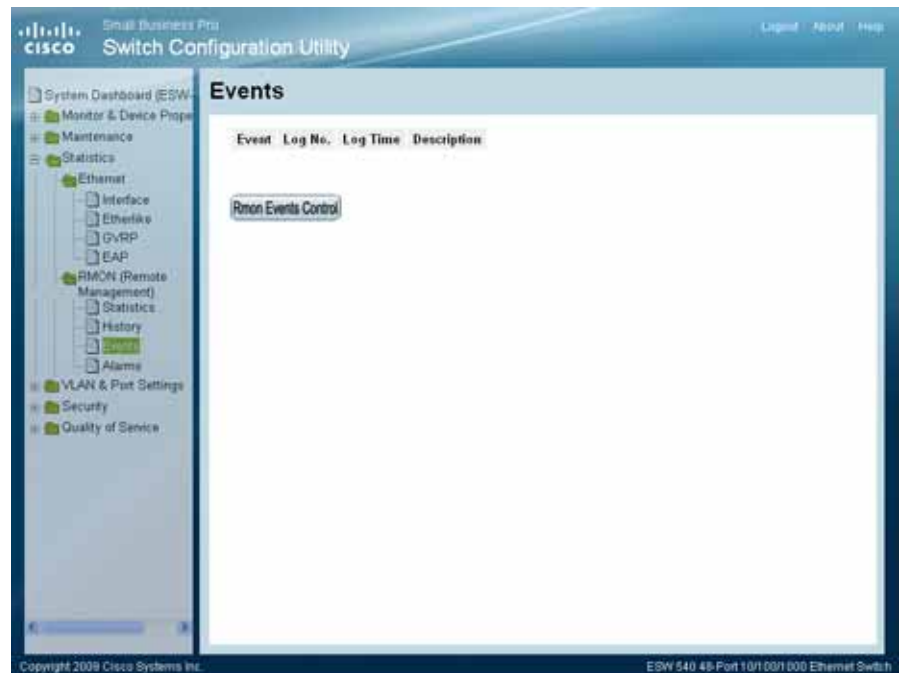
The *RMON Events Log Page* contains a list of RMON events.

**STEP 1** Click **Statistics > RMON (Remote Management) > Events**. The *RMON Events Page* opens:

**STEP 2** Click the **Events Log** button. The *RMON Events Log Page* opens:



## RMON Events Log Page



The *RMON Events Log Page* contains the following fields:

- **Event** — Displays the RMON Events Log entry number.
- **Log No.** — Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

To return to the RMON Events Page, click the **RMON Events Control** button.

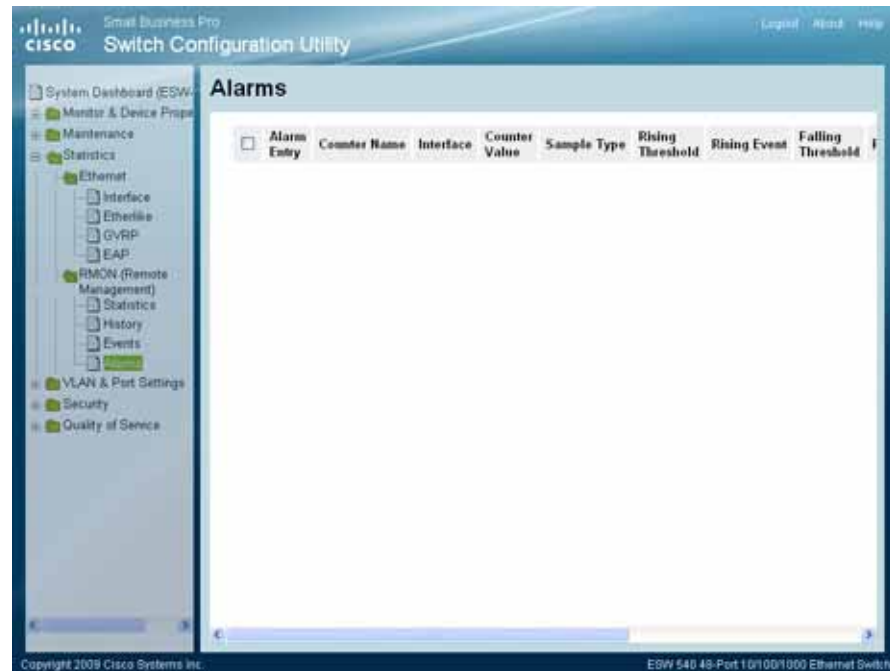
## Defining RMON Alarms

The *RMON Alarms Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

To set RMON alarms:

- STEP 1** Click **Statistics > RMON (Remote Management) > Alarms**. The *RMON Alarms Page* opens:

#### RMON Alarms Page



The *RMON Alarms Page* contains the following fields:

- **Alarm Entry** — Indicates the alarm entry number.
- **Counter Name** — Displays the selected MIB variable.
- **Interface** — Displays the interface (port or EtherChannel) for which RMON statistics are displayed. The possible field values are:
  - *Port* — Displays the RMON statistics for the selected port.
  - *EtherChannel* — Displays the RMON statistics for the selected EtherChannel.
- **Counter Value** — Displays the current counter value for the particular alarm.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

- *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising Event** — Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the RMON Events page.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
  - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
  - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
  - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval (Sec)** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

**STEP 2** Click the **Add** button. The *Add RMON Alarm Page* opens:

## Add RMON Alarm Page

**Add RMON Alarm**

Alarm Entry: 1

Interface: ☒ Port g1 ☐ EtherChannel 1

Counter Name: Total Bytes (Octets)- Receive

Sample Type: Absolute

Rising Threshold: 100

Rising Event:

Falling Threshold: 20

Falling Event:

Startup Alarm: Rising and Falling

Interval: 100

Owner:

Apply

The *Add RMON Alarm Page* contains the following fields:

- **Alarm Entry** — Indicates the alarm entry number.
- **Interface** — Displays the interface (port or EtherChannel) for which RMON statistics are displayed. The possible field values are:
  - *Ports* — Displays the RMON statistics for the selected port.
  - *EtherChannels* — Displays the RMON statistics for the selected EtherChannel.
- **Counter Name** — Displays the selected MIB variable.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
  - *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.

- **Rising Event** — Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
  - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
  - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
  - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The RMON alarm is added, and the device is updated.

## Modifying RMON Alarm Settings

**STEP 1** Click **Statistics > RMON (Remote Management) > Alarms**. The *RMON Alarms Page* opens:

**STEP 2** Click the **Edit** Button. The *Edit RMON Alarm Page* opens:

## Edit RMON Alarm Page

The screenshot shows the 'Edit RMON Alarm' configuration page. It contains the following fields and controls:

- Alarm Entry:** A dropdown menu with the value '1' selected.
- Interface:** Radio buttons for 'Port' (selected) and 'EtherChannel'. The 'Port' dropdown shows 'g3' and the 'EtherChannel' dropdown shows 'g1'.
- Counter Name:** A dropdown menu with 'Total Bytes (Octets)- Receive' selected.
- Counter Value:** A text input field.
- Sample Type:** A dropdown menu with 'Absolute' selected.
- Rising Threshold:** A text input field.
- Rising Event:** A dropdown menu with '1 - Default Description' selected.
- Falling Threshold:** A text input field.
- Falling Event:** A dropdown menu.
- Startup Alarm:** A dropdown menu with 'Rising Alarm' selected.
- Interval (Sec):** A text input field.
- Owner:** A text input field.
- Apply:** A button at the bottom right.

The *Edit RMON Alarm Page* contains the following fields:

- **Alarm Entry** — Indicates the alarm entry number.
- **Interface** — Displays the interface (port or EtherChannel) for which RMON statistics are displayed. The possible field values are:
  - *Port* — Displays the RMON statistics for the selected port.
  - *EtherChannel* — Displays the RMON statistics for the selected EtherChannel.
- **Counter Name** — Displays the selected MIB variable.
- **Counter Value** — Displays the current counter value for the particular alarm.
- **Sample Type** — Defines the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
  - *Delta* — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
  - *Absolute* — Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold** — Displays the rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.

- **Rising Event** — Selects an event which is defined in the Events table that triggers the rising threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Selects an event which is defined in the Events table that triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Page*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
  - *Rising Alarm* — The rising counter value that triggers the rising threshold alarm.
  - *Falling Alarm* — The falling counter value that triggers the falling threshold alarm.
  - *Rising and Falling* — The rising and falling counter values that trigger the alarm.
- **Interval** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The RMON alarms are modified, and the device is updated.

# Aggregating Ports

EtherChannels optimize port usage by linking a group of ports together to form a single aggregated group. EtherChannels multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.

The device supports both static EtherChannels and Link Aggregation Control Protocol (LACP) EtherChannels. LACP EtherChannels negotiate aggregating port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a EtherChannel between them. Ensure the following:

- All ports within a EtherChannel must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different EtherChannel.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the EtherChannel have the same ingress filtering and tagged modes.
- All ports in the EtherChannel have the same back pressure and flow control modes.
- All ports in the EtherChannel have the same priority.
- All ports in the EtherChannel have the same transceiver type.
- The device supports up to 64 EtherChannels, and eight ports in each EtherChannel.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured EtherChannel.
- Ports added to a EtherChannel lose their individual port configuration. When ports are removed from the EtherChannel, the original port configuration is applied to the ports.

This section contains information for configuring ports and contains the following topics:



- Defining EtherChannel Management
- Configuring LACP
- Defining EtherChannel Settings

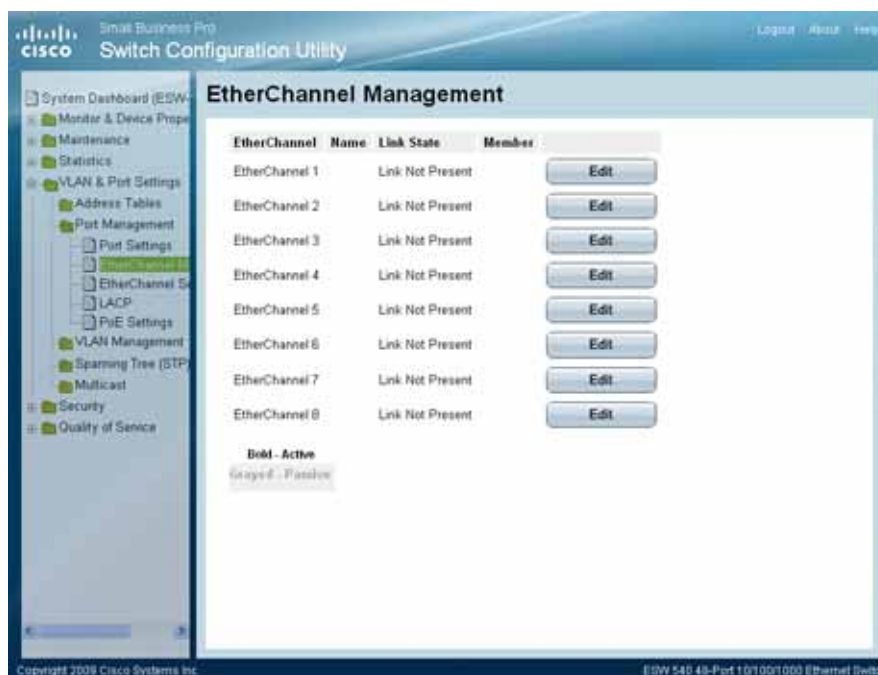
## Defining EtherChannel Management

Ports added to a EtherChannel lose their individual port configuration. When ports are removed from the EtherChannel, the original port configuration is applied to the ports.

To define EtherChannel management:

- STEP 1** Click **VLAN & Port Settings > Port Management > EtherChannel Management**. The *EtherChannel Management Page* opens:

### EtherChannel Management Page



The *EtherChannel Management Page* contains the following fields.

- **EtherChannel** — Displays the EtherChannel number.
- **Name** — Displays the EtherChannel name.

- **Link State** — Displays the link operational status.
- **Member** — Displays the ports configured to the EtherChannel.

### Modifying LAG Membership

**STEP 1** Click **VLAN & Port Settings > Port Management > EtherChannel Management**. The *EtherChannel Management Page* opens:

**STEP 2** Click the **Edit** button. The *Edit EtherChannel Management Page* opens:

### Edit EtherChannel Management Page

**Edit EtherChannel Management**

EtherChannel: 1

EtherChannel Name:

LACP: ☐

Port List: g1, g2, g3, g4, g5, g6, g7, g8

EtherChannel members:

>> <<

Apply

The *Edit EtherChannel Management Page* contains the following fields.

- **EtherChannel** — Displays the EtherChannel number.
- **EtherChannel Name** — Displays the EtherChannel name.
- **LACP** — Indicates that LACP is enable on the EtherChannel. The possible field values are:
  - Checked — Enables LACP on the EtherChannel.
  - Unchecked — Disables LACP on the EtherChannel. This is the default value.

- **Port List** — Contains a list of ports than can be added to a EtherChannel by using the >> button to add or the << button to remove items.
- **EtherChannel Members** — Displays the ports which are members of the selected EtherChannel.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The EtherChannel membership is defined, and the device is updated.

## Defining EtherChannel Settings

EtherChannels optimize port usage by linking a group of ports together to form a single aggregated group. EtherChannels multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.

The *EtherChannel Settings Page* contains fields for configuring parameters for configured EtherChannels. The device supports up to eight ports per EtherChannel, and eight EtherChannels per system. The device support Private VLAN Edge, which can be enabled for specific EtherChannels on the *Edit EtherChannel Settings Page*.

## Aggregating Ports

### Defining EtherChannel Settings

- STEP 1** Click **VLAN & Port Settings > Port Management > EtherChannel Settings**. The *EtherChannel Settings Page* opens:

#### EtherChannel Settings Page



The *EtherChannel Settings Page* contains the following fields:

- **Copy From Entry Number** — Copies the EtherChannel configuration from the specified table entry.
- **To Entry Number(s)** — Assigns the copied EtherChannel configuration to the specified table entry.
- **EtherChannel** — Displays the EtherChannel ID number.
- **Description** — Displays the user-defined port name.
- **Type** — Displays the port types that comprise the EtherChannel.
- **Status** — Indicates if the EtherChannel is currently operating.
- **Speed** — Displays the configured speed at which the EtherChannel is operating.
- **Auto Negotiation** — Displays the current Auto Negotiation setting. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, and flow control abilities to its partner.

## Aggregating Ports

### Defining EtherChannel Settings

- **Flow Control** — Displays the current Flow Control setting. Flow control may be enabled, disabled, or be in auto negotiation mode. Flow control operates when the ports are in full duplex mode.
- **PVE** — Indicates that this EtherChannel's ports are protected by an uplink, so that the forwarding decisions are overwritten by those of the ports that protect them.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The EtherChannel Settings are defined, and the device is updated.

### Modifying EtherChannel Settings

**STEP 1** Click **VLAN & Port Settings > Port Management > EtherChannel Settings**. The EtherChannel Settings Page opens.

**STEP 2** Click the **Edit** button. The *Edit EtherChannel Page* opens:

#### Edit EtherChannel Page

The screenshot shows the 'Edit EtherChannel' configuration page. It contains the following fields and controls:

- Ether Channel:** A dropdown menu with '1' selected.
- Description:** An empty text input field.
- Ether Channel Type:** A dropdown menu.
- Admin Status:** A dropdown menu with 'Up' selected.
- Current EtherChannel Status:** A dropdown menu.
- Reactivate Suspended EtherChannel:** An unchecked checkbox.
- Operational Status:** A dropdown menu with 'Active' selected.
- Admin Auto Negotiation:** A dropdown menu with 'Enable' selected.
- Current Auto Negotiation:** A dropdown menu.
- Admin Advertisement:** Radio buttons for 'Max Capability', '10 Full', '100 Full', and '1000 Full'. 'Max Capability' is selected.
- Current Advertisement:** A dropdown menu with 'Unknown' selected.
- Neighbor Advertisement:** A dropdown menu with 'Unknown' selected.
- Admin Speed:** A dropdown menu with '10M' selected.
- Current EtherChannel Speed:** A dropdown menu.
- Admin Flow Control:** A dropdown menu with 'Disable' selected.
- Current Flow Control:** A dropdown menu.
- PVE:** A dropdown menu with 'None' selected.
- Apply:** A button at the bottom right.

The *Edit EtherChannel Page* contains the following fields:

- **EtherChannel** — Displays the EtherChannel ID number.
- **Description** — Displays the user-defined port name.
- **EtherChannel Type** — Indicates the port types that comprise the EtherChannel.
- **Admin Status** — Enables or disables traffic forwarding through the selected EtherChannel.
- **Current EtherChannel Status** — Indicates if the EtherChannel is currently operating.
- **Reactivate Suspended EtherChannel** — Reactivates a port if the EtherChannel has been disabled through the locked port security option or through Access Control List configurations.
- **Operational Status** — Indicates whether the EtherChannel is currently operational or non-operational.
- **Admin Auto Negotiation** — Enables or disables Auto Negotiation on the EtherChannel. Auto-negotiation is a protocol between two link partners that enables a EtherChannel to advertise its transmission rate, and flow control (the flow control default is disabled) abilities to its partner.
- **Current Auto Negotiation** — Displays the current Auto Negotiation setting.
- **Admin Advertisement** — Specifies the capabilities to be advertised by the EtherChannel. The possible field values are:
  - *Max Capability* — Indicates that all EtherChannel speeds and Duplex mode settings can be accepted.
  - *10 Half* — Indicates that the EtherChannel is advertising a 10 Mbps speed and half Duplex mode setting.
  - *10 Full* — Indicates that the EtherChannel is advertising a 10 Mbps speed and full Duplex mode setting.
  - *100 Half* — Indicates that the EtherChannel is advertising a 100 Mbps speed and half Duplex mode setting.
  - *100 Full* — Indicates that the EtherChannel is advertising a 100 Mbps speed and full Duplex mode setting.
  - *1000 Full* — Indicates that the EtherChannel is advertising a 1000 Mbps speed and full Duplex mode setting.
- **Current Advertisement** — Indicates the admin advertisement status. The EtherChannel advertises its capabilities to its neighbor EtherChannel to start

the negotiation process. The possible field values are those specified in the Admin Advertisement field.

- **Neighbor Advertisement** — The neighbor EtherChannel (the EtherChannel to which the selected interface is connected) advertises its capabilities to the EtherChannel to start the negotiation process. The possible values are those specified in the Admin Advertisement field.
- **Admin Speed** — The configured speed at which the EtherChannel is operating.
- **Current EtherChannel Speed** — The current speed at which the EtherChannel is operating.
- **Admin Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the EtherChannel.
- **Current Flow Control** — The user-designated Flow Control setting.
- **PVE** — Indicates if this EtherChannel's ports are protected by an uplink, so that the forwarding decisions are overwritten by those of the ports that protect them.

## Configuring LACP

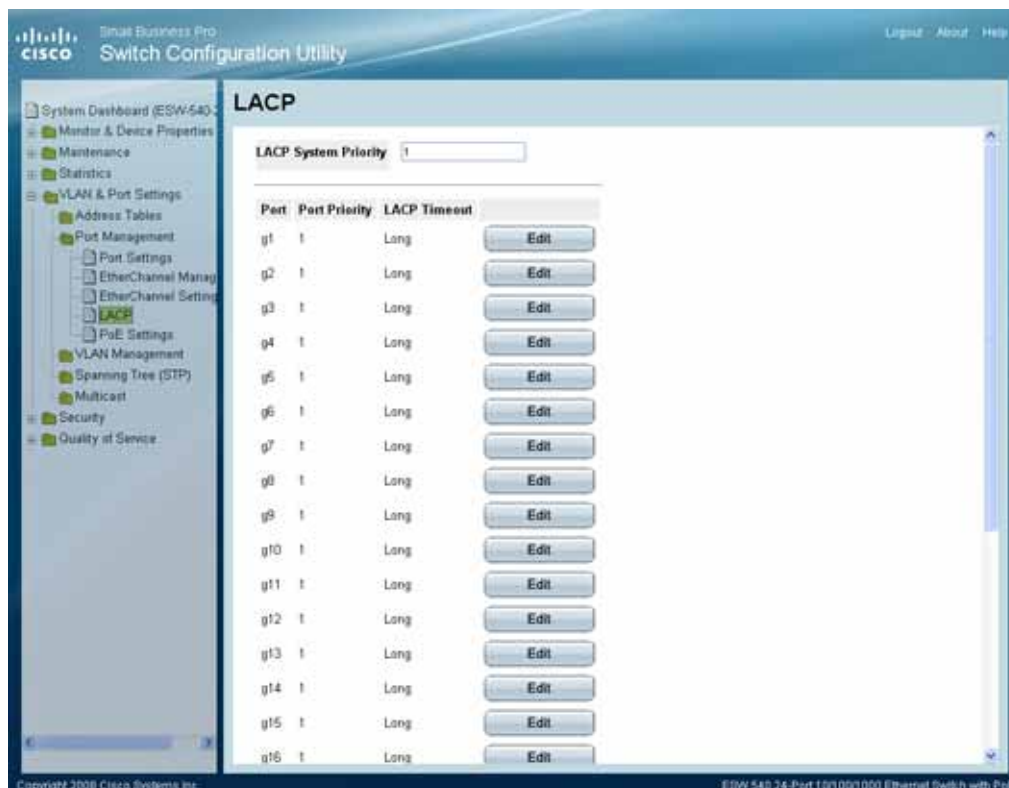
Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed, set to full-duplex operations.

Aggregated Links can be manually setup or automatically established by enabling Link Aggregation Control Protocol (LACP) on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.

To define LACP:

**STEP 1** Click **VLAN & Port Settings > Port Management > LACP**. The *LACP Page* opens:

#### LACP Page



The *LACP Page* contains fields for configuring LACP EtherChannels.

- **LACP System Priority** — Indicates the global LACP priority value. The possible range is 1- 65535. The default value is 1.
- **Port** — Defines the port number to which timeout and priority values are assigned.
- **Port Priority** — Defines the LACP priority value for the port. The field range is 1- 65535.
- **LACP Timeout** — Administrative LACP timeout. The possible field values are:
  - *Short* — Defines a short timeout value.
  - *Long* — Defines a long timeout value. This is the default value.

**STEP 2** Define the relevant fields.

**STEP 3** Click **Apply**. The LACP EtherChannels are defined, and the device is updated.

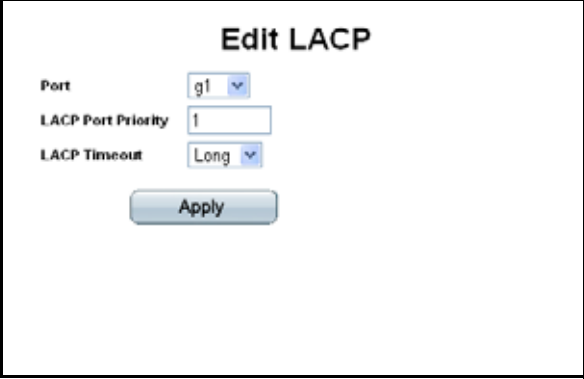


## Modify LACP Parameter Settings

**STEP 1** Click **VLAN & Port Settings > Port Management > LACP**. The *LACP Page* opens:

**STEP 2** Click the **Edit** button. The *Edit LACP Page* opens:

### Edit LACP Page

The screenshot shows a web interface titled "Edit LACP". It contains three configuration fields: "Port" with a dropdown menu showing "g1", "LACP Port Priority" with a text input field containing the value "1", and "LACP Timeout" with a dropdown menu showing "Long". Below these fields is a blue "Apply" button.

The *Edit LACP Page* contains the following fields:

- **Port** — Defines the port number to which timeout and priority values are assigned.
- **LACP Port Priority** — Defines the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Administrative LACP timeout. The possible field values are:
  - *Short* — Defines a short timeout value.
  - *Long* — Defines a long timeout value. This is the default value.

**STEP 3** Define the relevant fields.

**STEP 4** Click **Apply**. The LACP Parameters settings are modified, and the device is updated.

# Managing Device Diagnostics

This section contains information for running diagnostic procedures on the switch, and includes the following topics:

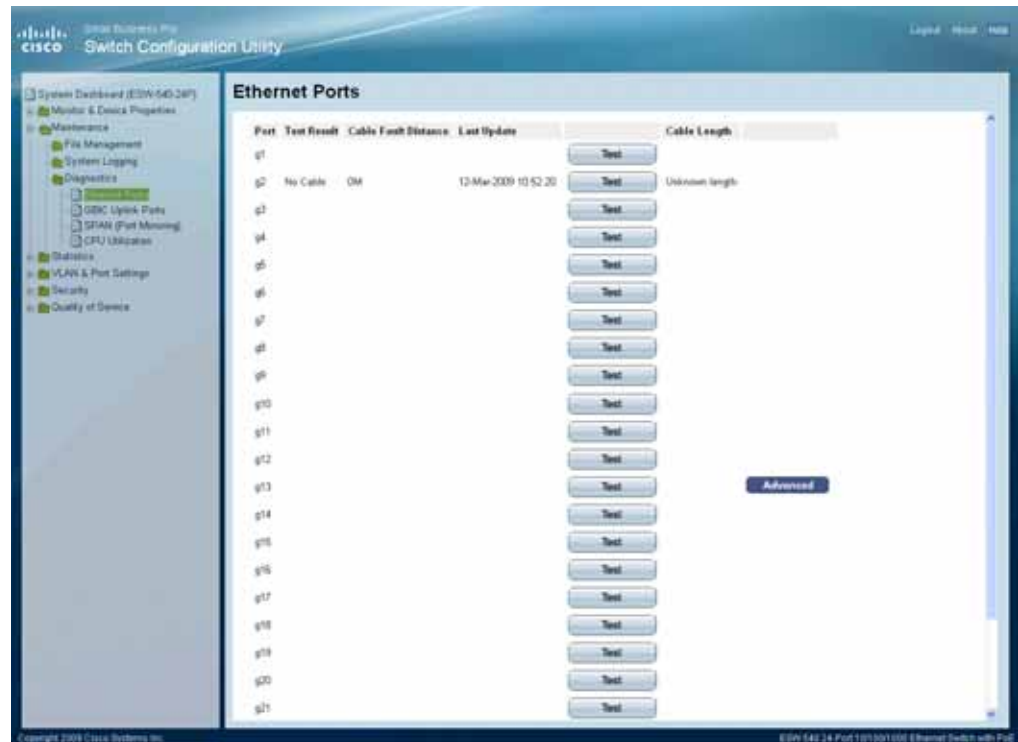
- Ethernet Ports
- GBIC Uplink Ports
- SPAN (Port Mirroring)
- CPU Utilization

## Ethernet Port Testing

The *Ethernet Ports Page* contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error that occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 100 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To test cables:

**STEP 1** Click **Maintenance > Diagnostics > Ethernet Ports**. The *Ethernet Ports* Page opens:

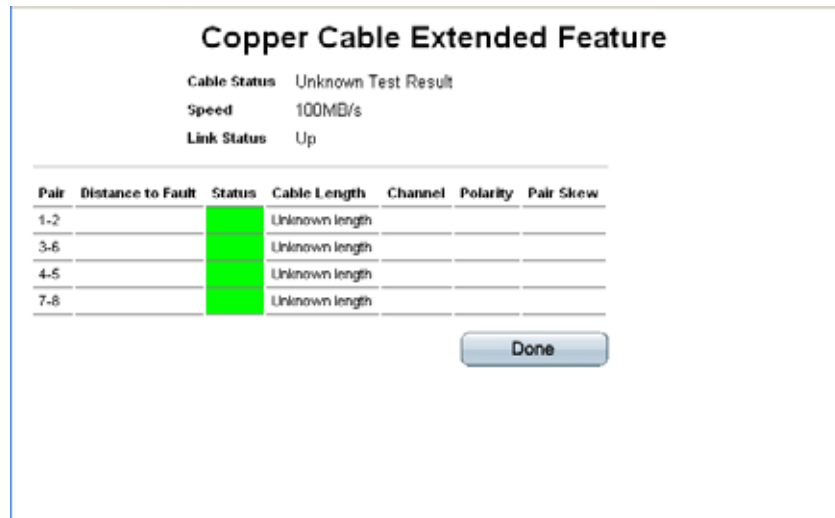


The Ethernet Ports Page contains the following fields:

- **Port** — Displays the port list.
- **Test Result** — Displays the cable test results. Possible values are:
  - *No Cable* — Indicates that a cable is not connected to the port.
  - *Open Cable* — Indicates that a cable is connected on only one side.
  - *Short Cable* — Indicates that a short has occurred in the cable.
  - *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred.
- **Last Update** — Indicates the last time the cable tests were updated.
- **Cable Length** — Indicates the cable length. This test can only be performed when the port is up and operating at 1 Gbps.

- STEP 2** Click the **Test** button to run the cable test. A popup message appears that states "The operation will shut down the tested port for a short period, continue?". Click **OK** to continue or **Cancel** to stop the test. The results of the test appear on the line associated with the port you tested.

Click on the **Advanced** button to open up the *Copper Cable Extended Feature Screen*.



**Copper Cable Extended Feature**

Cable Status: Unknown Test Result  
 Speed: 100MB/s  
 Link Status: Up

Pair	Distance to Fault	Status	Cable Length	Channel	Polarity	Pair Skew
1-2			Unknown length			
3-6			Unknown length			
4-5			Unknown length			
7-8			Unknown length			

Done

The *Copper Cable Extended Feature* page contains the following fields.

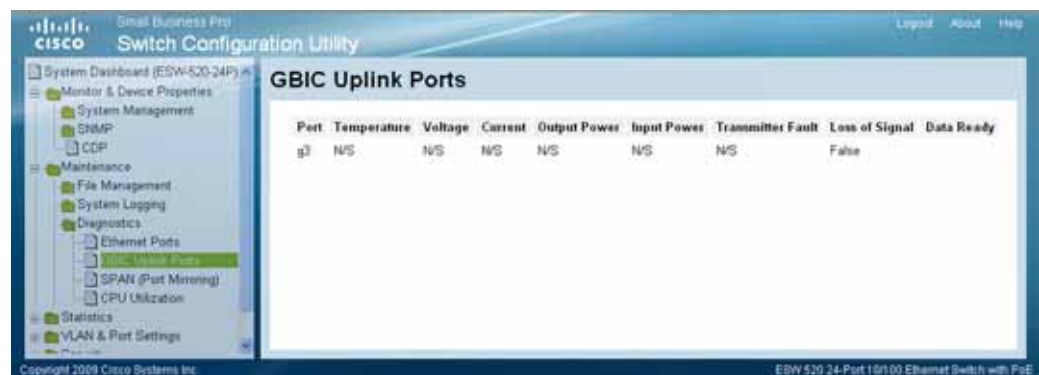
- **Cable Status** — Displays the cable status.
- **Speed** — Indicates the speed at which the cable is transmitting packets.
- **Link Status** — Displays the current link status.
- **Pair** — The pair of cables under test.
- **Distance to Fault** — Indicates the distance between the port and where the cable error occurred.
- **Status** — Displays the cable status.
- **Cable length** — Displays the cable length.
- **Channel** — Displays the cable's channel.
- **Polarity** — Automatic polarity detection and correction permits on all RJ-45 ports for automatic adjustment of wiring errors.
- **Pair Skew** — Reaction or transmission time in nanoseconds for the selected cable pair and given cable length.

**STEP 3** Click **Done** to close the window.

## Performing GBIC Uplink Testing

The *GBIC Uplink Page* allows network managers to perform tests on Fiber Optic cables. Optical transceiver diagnostics can be performed only when the link is present. During the port test, the port moves to a down state.

**STEP 1** Click **Maintenance > Diagnostics > GBIC Uplink Ports**. The *GBIC Uplink Ports Page* opens:



The *GBIC Uplink Ports* page contains the following fields:

- **Port** — Displays the port number on which the cable is tested.
- **Temperature** — Displays the temperature in Celsius at which the cable is operating.
- **Voltage** — Displays the voltage at which the cable is operating.
- **Current** — Displays the current at which the cable is operating.
- **Output Power** — Indicates the rate at which the output power is transmitted.
- **Input Power** — Indicates the rate at which the input power is transmitted.
- **Transmitter Fault** — Indicates if a fault occurred during transmission.
- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — Indicates the data status.

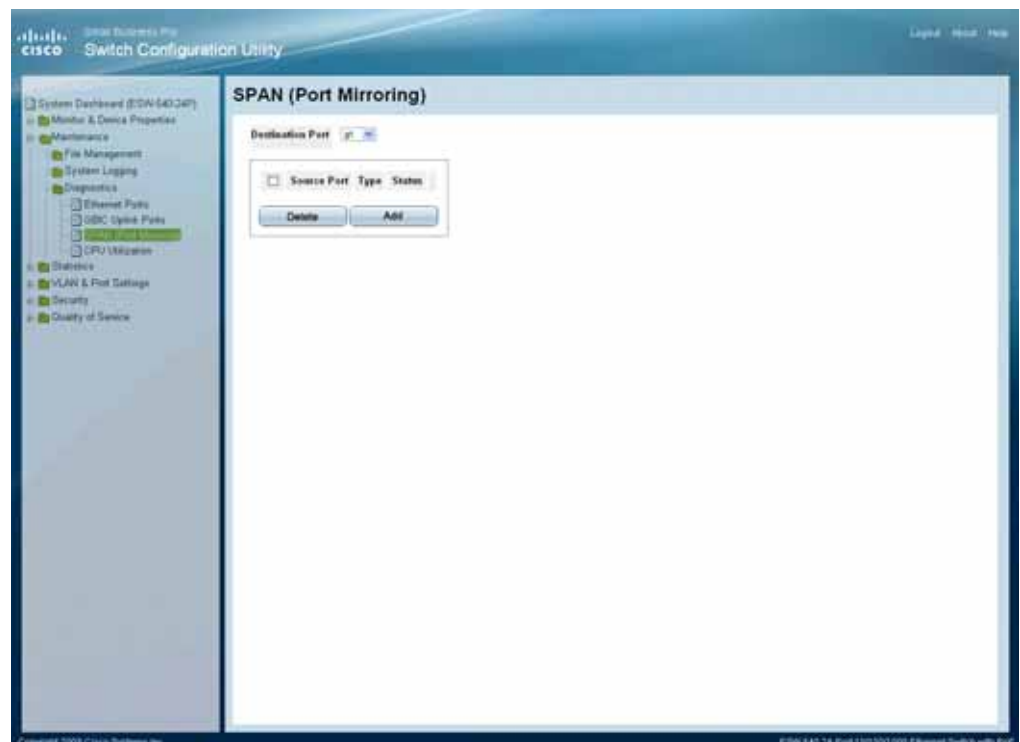
## Configure Span (Port Mirroring)

Port Mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as diagnostic tool and/or a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators configure port mirroring by selecting a specific port to copy all packets, and different ports from which the packets are copied.

To enable port mirroring:

- STEP 1** Click **Maintenance > Diagnostics > SPAN (Port Mirroring)**. The *SPAN (Port Mirroring)* Page opens:



The SPAN (*Port Mirroring*) page contains the following fields:

- **Destination Port** — Defines the port to which the source port's traffic is mirrored.



**NOTE** The destination port must be configured with a Smart Port role of "Other" using the Smart Port Wizard before configuring for port mirroring.

- **Source Port** — Defines the port from which traffic is to be analyzed.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  - *Rx Only* — Defines the port mirroring for receive traffic only on the selected port.
  - *Tx Only* — Defines the port mirroring on transmitting ports. This is the default value.
  - *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports.
- **Status** — Indicates if the port is currently monitored. The possible field values are:
  - *Active* — Indicates the port is currently monitored.
  - *NotReady* — Indicates the port is not currently monitored.

Click the **Add** button. The *Add Port Mirroring* page opens:

The screenshot shows a web interface titled "Add Port Mirroring". It contains two dropdown menus. The first is labeled "Source Port" and has "g1" selected. The second is labeled "Type" and has "Tx Only" selected. Below these fields is a button labeled "Apply".

The *Add Port Mirroring* page contains the following fields:

- **Source Port** — Defines the port from which traffic is to be analyzed.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  - *Rx Only* — Defines the port mirroring on receiving ports. This is the default value.

- *Tx Only* — Defines the port mirroring on transmitting ports.
- *Tx and Rx* — Defines the port mirroring on both receiving and transmitting ports.

**STEP 2** Define the relevant fields.

Click **Apply**. Port mirroring is added, and the device is updated.

---

To Delete an entry, click on the the selected entry in the table and then press **Delete**.

## Monitoring CPU Utilization

The *CPU Utilization* page contains information about the system's CPU utilization.



---

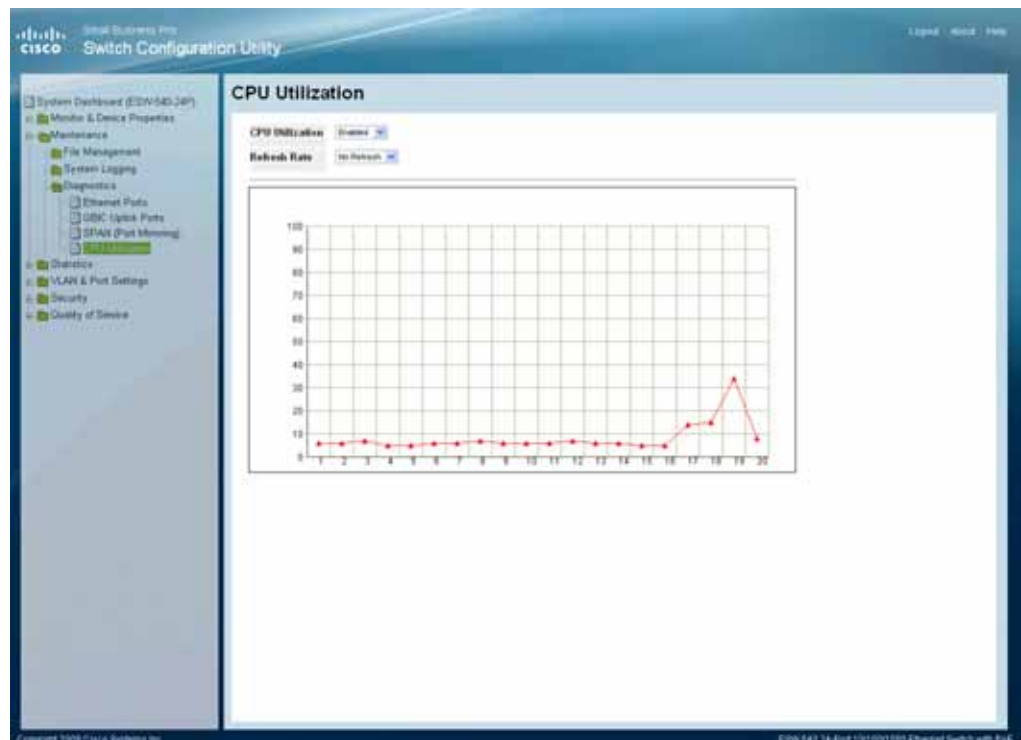
**NOTE** The CPU Utilization page requires that the Java applet be installed and properly configured prior to executing the test.

---

To observe the CPU Utilization:



- STEP 1** Click **Maintenance > Diagnostics > CPU Utilization**. The *CPU Utilization* Page opens:



The *CPU Utilization* page contains the following fields:

- **CPU Utilization** — Displays CPU resource utilization information. The possible field values are:
  - *Enabled* — Enables viewing CPU utilization information. This is the default value.
  - *Disabled* — Disables viewing the CPU utilization information.
- **Refresh Rate** — Amount of time that passes before the statistics are refreshed. The possible field values are:
  - *No Refresh* — Indicates that the CPU utilization statistics are not refreshed.
  - *15 Sec* — Indicates that the CPU utilization statistics are refreshed every 15 seconds.

- *30 Sec* — Indicates that the CPU utilization statistics are refreshed every 30 seconds.
  - *60 Sec* — Indicates that the CPU utilization statistics are refreshed every 60 seconds.
- **Usage Percentages** — Graph's y-axis indicates the percentage of the CPU's resources consumed by the device.
- **Time** — Graph's x-axis indicates the time, in 15, 30, and 60 second intervals, that usage samples are taken.